AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–765

FEDERAL BUREAU OF INVESTIGATION OVERSIGHT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JULY 27, 2005

Serial No. J–109–36

Printed for the use of the Committee on the Judiciary

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00001 Fmt 6011 Sfmt 6011 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

FEDERAL BUREAU OF INVESTIGATION OVERSIGHT

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00002 Fmt 6019 Sfmt 6019 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

S. HRG. 109–765

FEDERAL BUREAU OF INVESTIGATION OVERSIGHT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JULY 27, 2005

Serial No. J–109–36

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

46–051 PDF WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00003 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

COMMITTEE ON THE JUDICIARY

ARLEN SPECTER, Pennsylvania, *Chairman*

ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
JOHN CORNYN, Texas
SAM BROWNBACK, Kansas
TOM COBURN, Oklahoma

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois

DAVID BROG, *Staff Director*
MICHAEL O'NEILL, *Chief Counsel*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00004 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Grassley, Hon. Charles E., a U.S. Senator from the State of Iowa, prepared statement	297
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	2
prepared statement	311
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania	1

WITNESSES

Fine, Glenn A., Inspector General, Department of Justice, Washington, D.C.	36
Hamilton, Lee H., President and Director, Woodrow Wilson International Center for Scholars, Washington, D.C.	38
Mueller, Robert S., III, Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C.	9
Russack, John A., Program Manager, Information Sharing Environment, Director of National Intelligence, Washington, D.C.	44
Webster, William H., Partner, Milbank, Tweed, Hadley & McCloy LLP, Washington, D.C.	40

QUESTIONS AND ANSWERS

Responses of Director Mueller to questions submitted by Senators Specter, Leahy and Feingold	54

SUBMISSIONS FOR THE RECORD

Fine, Glenn A., Inspector General, Department of Justice, Washington, D.C., prepared statement	275
Hamilton, Lee H., President and Director, Woodrow Wilson International Center for Scholars, Washington, D.C., prepared statement	299
Mueller, Robert S., III, Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C., prepared statement	315
Russack, John A., Program Manager, Information Sharing Environment, Director of National Intelligence, Washington, D.C., prepared statement	324
Webster, William H., Partner, Milbank, Tweed, Hadley & McCloy LLP, Washington, D.C., prepared statement	327

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00005 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

FEDERAL BUREAU OF INVESTIGATION OVERSIGHT

WEDNESDAY, JULY 27, 2005

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 9:32 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Arlen Specter, Chairman of the Committee, presiding.

Present: Senators Specter, Grassley, DeWine, Sessions, Cornyn, Leahy, Biden, Kohl, Feinstein, Feingold, Schumer, and Durbin.

OPENING STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA

Chairman SPECTER. Good morning, ladies and gentlemen. The Judiciary Committee will now proceed with our oversight hearing on the Federal Bureau of Investigation.

Before proceeding to the hearing at hand, I thought it would be useful to make a comment or two about the scheduling on the confirmation hearings of Judge Roberts. I had sent word to Senator Leahy earlier this morning that I wanted to spend a few minutes on that subject because we were being questioned about it incessantly. And Senator Leahy and I since the middle of last week, right after the appointment, have been talking about it repeatedly to try to work out an agreeable schedule. I compliment the distinguished Ranking Member for his cooperation and the way we have worked together in processing the work of the Committee, and to the maximum extent possible, that is what we want to continue to do.

We have an obligation, as I see it, to finish the confirmation hearing so that the nominee is in place, if he is confirmed, on the first Monday in October, which is October the 3rd.

My preference has been to start in September, but I have said from the outset that so far as I was concerned, I was flexible on the subject as to either August or September, depending upon all the circumstances. Notwithstanding the preference which I have expressed, I believe there is a duty to start the hearings at a time best calculated to finish by the October 3rd date.

I talked to Senator Leahy yesterday repeatedly and posed the question: Is it realistic to get a commitment that we will vote on Judge Roberts by September 29th? And absent that commitment, it seems to me that we have to start in August, on August 29th. And it may be that we cannot finish by October 3rd starting on August 29th. There are too many imponderables which we have seen,

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00007 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

and the Senate in large measure functions on what each individual Senator is willing to do. And one Senator can throw a monkey wrench into the process, and we have seen from experience—Senator Leahy has been involved in ten confirmation hearings and I have been involved in nine; Senator Grassley has been involved in nine—that there are many unpredictable things which arise.

We have already had discussions about reviewing the records, and I note yesterday that the eight Democrats on the Committee sent a letter to the White House, which I am not at all critical of. I think it is perfectly appropriate. But that sort of represents the differing views which Pat Leahy and Arlen Specter will have no matter how closely we coordinate. And we cannot control our committees. We cannot control our caucuses. All we can do is our very best.

But the nub of my conclusion is that duty comes ahead of preference, and unless there is a commitment—and, again, I repeat, I am not asking for a commitment because I do not think it is realistic to get a commitment, because if Pat and I could solve it, we have no problems. We would come to terms promptly. But we do not control the whole situation. But absent that kind of a commitment, it seems to me that duty will call on us to go ahead with August 29th.

Let me yield to my distinguished Ranking Member now.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Again, I think if it was Senator Specter and myself, we could easily work this out. We could easily do it in September. I still think that is the better course. One, just a purely personal thing is that we have—it is not the members of this Committee will be back here in August, but there are dozens upon dozens—actually hundreds of people who work for the Senate, staff and so on, hundreds of members of the press, others who have determined that as a time that is always open, a time they could take their children back to school, a time they could actually spend time with their families.

When I first came to the Senate, the only time you had a recess that you could count on was in the winter months because many of the older members wanted to go off to warmer climes. Of course, that did nothing for those with children.

We then around the time I came to the Senate initiated the idea of having an August break, and it is the one time where families with children—and not only members but the hundreds upon hundreds of staff who work here—could plan time to actually be with their children. And the staff members work a lot later than we do. The press and everybody else could plan on that time. I think that that is something we ought to be considering if this is going to be a family-friendly Senate, as we have been promised it would be, or not.

We are talking about somebody who is going to serve, if confirmed, to the year 2030, 2040. To spend a few days longer to make sure we do it right does not create a problem in my mind. If somebody is going to be there to the year 2030 to 2040, a few days one

way or the other to make sure we get it right makes some sense to me.

Now, I am convinced today, with the record we have before us, that there will be a vote by the end of September. The irony is the vote will probably be the exact same day, whether we hold a hearing in August or whether we hold a hearing in September. The difference is, of course, families' lives would be disrupted substantially in August. They would not be disrupted as much in September. But the end result would be the same. And for the life of me, I cannot understand why we should not do it this way.

Now, we have worked cooperatively, and I commend the Chairman. As he knows, if the other party has to be in control, there is nobody I would rather have as Chairman than he. He has handled this as the smartest lawyer in the U.S. Senate, as he is. He has also handled this in the best manner of the bar to make sure we do it right. But I do worry that there are those special interest groups on the right and the left who want to make a game out of this when, after all, it is only the members of this Committee that are going to have the initial vote. I worry that—I saw a comment by the White House press secretary today suggesting that it is outrageous I might want to see something the President has not even read.

Now, I know that the White House press secretary much prefers talking about Karl Rove, but I would suggest to him that that is probably an unrealistic standard to set, that I can only read things that the President has read, because I doubt very much the President, whom I respect greatly, has read Judge Roberts's opinions, to give you one example. I intend to read all of Judge Roberts's opinions. I do not expect the President has read all of Judge Roberts's opinions, nor would I expect him to. But these are the kinds of semantic games that we ought to leave to the side. Let the Chairman and me work this out.

So I would again hope that we would start in September. You know, the Republicans control the Senate and, of course, they can decide to do it in August. I think it will give the impression that we are rushing to something before we are even prepared to go to a hearing. And it would also, of course, disrupt many, many, many hundreds of families if we do it that way. The irony is the final vote will still be on the same day, whether we do it in August or whether we do it in September.

So I wish all the conflicting groups would back off, including the Senate leadership and the White House, and let Chairman Specter and me work this out. I have an enormous amount of respect for the Chairman. He keeps his commitments to me and to others. I think if it is left to us, we will have a hearing the Senate can be proud of.

Chairman SPECTER. Thank you very much, Senator Leahy.

Just one final word. We are very much aware of the commitments made in August, and in making this statement with all the staff here, I thought it would be better if the staff heard it from the Chairman and the Ranking Member than just reading about it in the newspapers and having a feel for what we are doing and what we are trying to accomplish. If we adjourn on the 29th of July, we will have 31 days until August the 29th. That does not

alter my preference, nor does it alter my duty. And Senator Leahy may be exactly right that we may vote on the same date no matter when we start. And I am not unaware that around here you get a lot more done customarily in 3 hours cooperatively than in 3 days or 3 weeks. But at the same time, that extra week could be determinative, and that is what is on my mind.

Thank you for coming in, Director Mueller, and the indulgence of everyone in talking about the Roberts hearing, which is sort of taking a lot of—the whole Roberts proceeding is sort of taking a lot of oxygen out of Washington. But the number one problem in America and the world remains terrorism, and the issue of avoiding another attack is the most important issue facing the Government of the United States to protect its people.

We have met with Director Mueller on a number of occasions to talk about the changes which have been going on in the FBI to see what is happening. We all know that there were many signals before Director Mueller's watch which were not focused on: the Phoenix report, the Minneapolis report with Coleen Rowley, the wrong standard for probable cause, the information on Zacarias Moussaoui, the information that the CIA had about terrorists in Kuala Lumpur not passed on to Immigration. And we are all as determined as we can be to avoid that happening again. But it is going to take a lot of hard work, and a lot has already been done.

This is the first in a series of oversight hearings. There have been very strong criticisms by both the Weapons of Mass Destruction Commission and the 9/11 Commission. The WMD Commission found resistance to cultural changes as the FBI transitions to a "hybrid law enforcement and intelligence agency." The WMD Commission was critical about the FBI still putting law enforcement ahead of intelligence gathering. The Commission noted that the Counterterrorism Directorate has seen six directors since September 11th, and the New York field office, where much of the FBI's counterterrorism efforts have been focused, has seen five directors since 9/11. Those are not encouraging signs.

The WMD Commission concluded that the FBI "is still far from having a strong analytical capability to drive and focus the Bureau's national security work." Nearly one-third of the FBI's intelligence analyst jobs remained unfilled in 2004 because of rapid turnover and other problems. The 9/11 Commission found that 66 percent of the FBI's analysts were not qualified to perform analytical duties.

That is just the top of the iceberg, and I will put the rest in the record in order to save time and stay within my opening statement 5-minute limit. There were faults found on the intelligence operations, and then you have the issue of technology, a subject that I personally have discussed in some detail with Director Mueller. And when you take a look at the Virtual Case File system, part of the FBI's technology modernization product intended to replace the Bureau's obsolete case management system, after spending 3 years and $170 million on the Virtual Case File system, the FBI declared it to be a complete failure.

Director Mueller, we appreciate what you are doing, and we have great confidence in you personally. And it is a gigantic task, and we want to be helpful to you. But there has to be some way to

move through the tangle of problems because of the intensity and importance of our duty to prevent another attack and to be in a position to put all the pieces together. And had all of the so-called dots been on one format, I think 9/11 could have been prevented. And I know that is your most fervent wish and what you are working for, as are we.

My red light has not gone on yet—there it goes.

Senator Leahy?

Senator LEAHY. Thank you, Mr. Chairman. I am glad you are holding this. I think it is a good hearing to continue our oversight. I welcome Director Mueller and the others, and I appreciate the time I spent with the Director a couple weeks ago. We went into this in some detail.

As he knows, I mentioned the FBI translation program. I have been following this for years. I authored the PATRIOT Act provision aimed at facilitating the hiring of more translators at the FBI. The Inspector General this morning released an update to its 2004 audit of the translation program. He gives credit where credit is due, says the FBI is making progress. I know that the Bureau is working hard to address this talent. I am frustrated, however, that it takes the Bureau on average 16 months to hire contract linguists.

I am aware of the number of hours of unreviewed counterterrorism audio is increasing. I know all of have this horrible sinking feeling, what happens if there are plans for an impending attack and we do not translate the audio until some time after the attack? None of us want that. I know that the Director does not. But I worry that we are not moving fast enough to get those translated. All of us want to see this program succeed. Everybody on this Committee does.

The FBI is the lead agency responsible for the Terrorist Screening Center. It made significant progress, but the Inspector General shows that their operations have been hampered by inadequate training and rapid turnover among the employees staffing the 24-hour call center, and, of course, deficient technology.

They were charged with what I think was an enormously difficult charge of consolidating 12 terrorist watch lists, but we have seen what happens when inaccuracies come in there. We have heard stories of planes being diverted because terrorist suspects on the no-fly list were allowed to board the airplane. If a person is so dangerous that he or she is properly on a no-fly list, then mid-flight is much too late to respond. On the other hand, we have seen so many people that they or their children might have the same name and are constantly being stopped—people that have had top secret clearance, people who have had distinguished military careers, Senator Kennedy. Of course, these Irish terrorists all look alike, but Senator Kennedy has been stopped numerous times from going on the same flight that he has been taking for 30 years because he is on a no-fly list.

That does not give me a great deal of confidence that we are necessarily getting the right people. It is also, of course, horribly disruptive to people who get their name on there by mistake and then cannot get their name off. If they have a business where they have

to travel around the country, they are loyal Americans losing their livelihood.

I am displeased with the FBI's handling of the Virtual Case File. The Chairman has already talked about it, but I feel they have bit off more than they can chew. They did not develop a finite and final list of project requirements, and they poorly chose to issue a contract without putting penalties in there. But what really bothered me is that the Congress, and this Committee in particular, was not given the full story of how poorly the project was progressing until it collapsed under its own weight. Not only are we out well over $100 million, but we are out several years of time, precious time that was lost, when we should be fighting terrorism.

I am disturbed by recent reports from GAO that an audit of the project has been substantially delayed because the FBI has taken weeks to schedule meetings and months to produce documents. I think there should be a lot fuller cooperation by the FBI with the GAO. They are not your enemy. They are your friends.

With respect to the VCF's replacement program, I did ask the Director at a recent hearing about costs. He said he would rather discuss the issue in private citing procurement sensitivities. When we talked in private, he still did not want to reveal those figures. I would just state this: There have been figures in the media. I have not been able to get them. Somehow the media has had some figures. I can tell you right now that if the costs are anywhere near what the media is reporting, I think you are going to have a real problem with this Committee.

So a lot has been undertaken since September 11th. The threats have changed. The Bureau is adjusting in several key areas. They have made some significant strides. I do want to underscore that. There is a lot of work to be done. We are not the enemy up here, even though some feel we are. We really do want to work together. This Committee has given an enormous amount of money, authorized an enormous amount of money for the FBI to make it better.

Thank you, Mr. Chairman.

[The prepared statement of Senator Leahy appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Senator Leahy.

We are going to proceed out of order because Senator Grassley chairs the Finance Committee and has a very pressing duty and is going to have to depart. He has been on this Committee since elected in 1980, sat next to me all that time. Quite a burden for Senator Grassley. And as I have just whispered to him and will repeat out loud, nobody has been more diligent on FBI oversight in the 25 years we have been here than Senator Grassley has. I may be second or may not be second, but there is no doubt that Senator Grassley is first.

Senator Grassley?

Senator GRASSLEY. Thank you very much.

Director Mueller, maybe it is not fair for me to go first because you may have had something in your opening statement that would satisfy me, but I do have to chair the hearing.

I have been asking a lot of questions about terrorist fund raising cases that have been developed by the Immigration and Custom Enforcement there in Houston, and so far your headquarters at

FBI and the field office at Houston have been giving contradictory answers. Essentially they have been pointing fingers at each other. Headquarters has blamed the field for mishandling the case, and the field has not accepted the blame. And since the FBI has refused to provide access to additional witnesses who might clear up the contradictions that are very obvious, how do you propose to resolve the conflicting statements? I think you are in a position to do it. They need to be resolved. And if it is determined that someone put the FBI's interest in turf battles ahead of the fight against terror, what would you do to hold that person accountable?

Mr. Mueller. Southeastern, we have had discussions on this, and I know our staffs have had lengthy discussions, and I am also well aware of your interest. It appears to be a difference of recollection between at least two individuals that is irreconcilable. It is a difference in recollection relating to the timing of bringing information together in order to undertake an application.

We take full responsibility for that delay. There was a delay. The difference in the timing I think was somewhat—in terms of the difference in recollection as to the timing, it is inconsequential in the sense that there was a delay; there should not have been a delay. My expectation is that as a result of this, we will not see this occurrence again. We have put into place procedures to assure that it does not happen. I do think it was a unique case, a unique set of circumstances, but we are determined that these circumstances not repeat themselves.

There was a delay in putting together information from two areas. It should have been put together sooner. Ultimately, I believe that the appropriate action was taken and that the case is ongoing with the full support of both agencies.

Senator GRASSLEY. Director Mueller, I think it is difficult maybe for you to solve this. I can solve it if I just get a chance to see the people I want to see and question the people I want to question. And I think that that is only fair that we get to the bottom of this, and I think it is part of Congressional oversight to get the job done. I think it is a help to you, and I think we need to get to the bottom of it.

On another matter, more than a month ago I had the opportunity to write the attorney for Basam Yusef, an Arab-American agent who is suing the FBI for discrimination, to request that he meet with my staff to provide information about problems in the Counter terrorism Division. His attorney sought permission from the FBI, but has not been given a clear answer on this. Given the FBI's recent attempt to fire another agent, Bob Wright, Mr. Yusef is afraid to honor my request without clear permission from the FBI.

We need a clear answer. Will you allow Mr. Yusef to meet with staff or not? And can you assure me that if Mr. Yusef complies with my request that the FBI will not retaliate against him? What we need is the cutting through of red tape within the FBI to get answers to our questions about whether or not this person can meet with my investigative staff, and we need this red tape cut crossways, not lengthways.

Mr. Mueller. Well, Senator, I think you are aware that I have been, I believe, cooperative in allowing persons to talk to your of-

fice. There is a protocol that one has to go through that gives some assurance that issues that are classified will be and continue to be appropriately classified. I would be happy to go back and see where we are in that process.

You alluded in your statement to the recommendation with regard to Robert Wright. As I believe I explained to you, I am concerned about allegations of retaliation. I requested that the Justice Department do the investigation in the allegations he raised. When that came back to us, there were additional concerns that we had. We made a recommendation. But I think I bent over backwards in allowing Mr. Wright to appeal that recommendation to the Department of Justice.

I can assure you that we will not retaliate against Mr. Yusef, have not retaliated against Mr. Wright, and have bent over backwards to give the actuality and, indeed, including the appearance of fairness. I know that you have the letter that was sent by us explaining to Mr. Wright the circumstances under which we made that recommendation, which we believed to be appropriate but we have given him that additional right to appeal to an independent outside arbiter.

Senator GRASSLEY. Well, then you are going to look at my opportunity to see Basam Yusef without retaliation?

Mr. Mueller. Yes, absolutely. I can assure you there will be no retaliation. The circumstances under which the discussion is had, I will have to review where we are in that process.

Senator GRASSLEY. Thank you.

Chairman SPECTER. Thank you very much, Senator Grassley.

Just one concluding note. Senator Grassley and I are the two survivors of 16 Republicans elected in 1980, the last two. We have Senator Dodd on the Democratic side, but it is a small group which remains.

Thank you very much, Senator Grassley, and without objection, we will put your opening statement in the record.

Senator GRASSLEY. Thank you.

[The prepared statement of Senator Grassley appears as a submission for the record.]

Chairman SPECTER. We turn now to Director Mueller for his opening statement, really an extraordinary record, educational background, professional background, public service, graduate of Princeton University, 1966, international relations from New York University in 1967, law degree from the University of Virginia, served as an officer in the Marine Corps, led a rifle platoon in Vietnam, recipient of the Bronze Star, two Navy commendation medals, the Purple Heart, and the Vietnam Cross of Gallantry.

Professionally, his career has been equally extraordinary, was United States Attorney in both the Northern District of California and in Boston, served as Acting Deputy Attorney General right before he became the FBI Director. And I think perhaps most noteworthy of his entire career, after having held lofty positions, he returned to public service as a senior litigator in the homicide section of the District of Columbia U.S. Attorney's Office, which is really remarkable, attesting to the fact that the best job, notwithstanding all these fancy titles, is being an assistant prosecutor.

Director Mueller, thank you for the job you are doing, and we look forward to your opening statement.

STATEMENT OF ROBERT S. MUELLER III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Director MUELLER. Thank you, Mr. Chairman, and thank you for having me here today. As you well know, having been one yourself, that is the best job one can have as an assistant prosecutor, particularly doing a service in cases that are so meaningful—

Chairman SPECTER. Senator Leahy just leaned over and said he agrees.

Director MUELLER. Another assistant prosecutor.

Thank you for allowing me to appear before you today, and let me start by updating you on recent changes within the FBI and additional changes that we anticipate in the near future.

Let me start by recognizing that last month the President announced that he had approved certain recommendations of the WMD Commission. And while the Commission had recognized in its report that we have made substantial progress in building our intelligence program, as I believe, Mr. Chairman, you pointed out, it expressed concern that our existing structure did not give the Director of National Intelligence the ability to ensure that our intelligence functions are fully integrated into the intelligence community.

At the direction of the President, we are currently prepared a plan to implement a national security service within the FBI. While the details of this plan are currently being discussed with both the Department of Justice and the Office of the DNI, I would like to share with the Committee the broad concepts under which this service is being developed.

One of our guiding principles since September 11th has been that the FBI's intelligence program be integrated with our investigative missions, and our FBI national security service will build on the progress of the Directorate of Intelligence and further promote this integration.

The integration of our intelligence and investigative missions ensures that intelligence drives our investigative as well as our intelligence operations. And this integration enables the FBI to capitalize our capability, our capacity to collect information and to extend that strength to the analysis and production of intelligence.

The national security service and intelligence service will be put together by combining our counterterrorism and counterintelligence components, and put it together with our Intelligence Directorate under the supervision of a single official who will report to the Deputy Director and to myself.

The development of a specialized national security workforce is a key component of this new service, and we will develop this workforce through initiatives, many of which are already in place, but those initiatives are designed to recruit, hire, train, and retain investigative and intelligence professionals who have the skills necessary to the success of our National intelligence, national security programs.

Finally, the creation of a national security within the FBI will enhance our ability to coordinate our National security activities with the DNI and with the rest of the intelligence community. The single FBI official in charge of the service will be able to ensure that we direct our National security resources in coordination with the DNI and the Attorney General. Also, as we all know, the DNI will also have authority to concur in the appointment of this official.

Mr. Chairman, this is a very broad outline of our plans for a national intelligence service within the FBI, and I am happy to provide the Committee with additional details as the implementation of this initiative progresses.

Mr. Chairman, you mentioned the Foreign Language Program, as has Senator Leahy. Let me just comment, if I could, on the findings of the Inspector General in this regard.

We welcome the input of the Inspector General. His findings have been exceptionally helpful in giving us guidance on where we need to improve, and I want to say that I appreciate the work that he spends and the guidance that he gives.

I will tell you that prior to September 11, 2001, translation capabilities, like many of our other programs, were decentralized and managed in the field. Since September 11th, we have established a Language Services Translation Center at FBI headquarters to provide centralized management of the Foreign Language Program. This provides a command and control structure at headquarters to ensure that our translator resource base of over 1,300 translators, distributed across 52 field offices, is strategically aligned with the priorities set out by our operational divisions and with the national intelligence priorities.

We have now integrated Language Services into the Directorate of Intelligence. This integration fully aligns our FBI foreign language and intelligence management activities across all of our field offices.

We, in addition, have instituted a prioritization process to ensure that foreign language collection is translated in accordance with a clear list of priorities. The Foreign Language Program receives regular weekly updates to FISA prioritization, and we are careful to ensure that the FBI's priorities are consistent with those of the intelligence community.

I know, as you mentioned, Senator Leahy, you and we are concerned whenever there is a backlog, and the report of the Inspector General indicates a current backlog. I will tell you that we have triaged and prioritized so that we have our highest priority counterterrorism intelligence intercepts reviewed generally within 24 hours. And this prioritization and triage process has helped us to reduce that accrued backlog.

As to that accrued backlog, if you review it you will see that much of it is what is called white noise from microphone recordings, and there is another piece of that backlog that is attributable to highly obscure languages and dialects that we are working hard to recruit translators to address.

Mr. Chairman, I would also like to address some of the Inspector General's concerns about our hiring and vetting of linguists. Since September 11th, we have recruited and processed more than

50,000 translator applicants. These efforts have resulted in the addition of 877 new contract linguists and another 112 language analysts, less the attrition. The FBI has increased its overall number of linguists by 69 percent with the number of linguists in certain high priority languages, such as Arabic, increasing by more than 200 percent.

At the same time, however, we must ensure translation security and quality. All FBI translator candidates are subject to a pre-employment vetting process that eliminates almost 90 percent of those who apply.

I will tell you that more than 95 percent of the FBI linguists are native speakers of their foreign language and hold Top Secret security clearances. Their native-level fluencies and long-term immersions within a foreign culture ensure not only a firm grasp of colloquial and idiomatic speech, but also of heavily nuanced language containing religious, cultural, and historical references. Beyond these qualities, over 80 percent of our FBI linguists hold at least a bachelor's degree and 37 percent hold a graduate-level degree. These qualities make them extremely valuable to the FBI's intelligence program, but also, unfortunately, particularly attractive to other employers who are seeking these scarce skill sets.

Mr. Chairman, we recognize that the FBI's Foreign Language Program is essential to our success, and we appreciate the oversight by the Committee. We appreciate the Inspector General indicating we have made progress. We understand that we have to make more progress and believe we are on track to do in those areas pointed out by the Inspector General.

Let me spend just a moment, Mr. Chairman, on technology.

As you or as anybody who looks at the intelligence community, indeed, the law enforcement community, we recognize the importance of collecting, analyzing, and disseminating information both internally and with other intelligence and law enforcement agencies. We have made since September 11th modernization of our information technology a top priority and have developed, I believe, in the last 2 years a coordinated, strategic approach to information technology under the centralized leadership of the Office of Chief Information Officer.

I will not go into the details because my prepared statement covers much of that, but I do want to point out that our proposed information management system, which we call Sentinel, is a form of a "service-oriented architecture," which is a suits of services geared to evolve with our new and emerging needs. This Sentinel project differs in many respects from Virtual Case File in that it will serve as the platform from which services can be gradually deployed, each deployment offering added improvements. Sentinel will pave the way, starting with our legacy case management system, for subsequent transformation of all legacy applications to modern technology under our enterprise architecture.

As we briefed the staff yesterday, the staff of the Judiciary Committee, and as I believe they heard, we are planning to deploy Sentinel in four phases over the next 40 months. I know that, as Senator Leahy pointed out, he is interested in the total cost of the Sentinel program. I must say that at this time cost estimates are considered "source selection information" as defined by the Federal Ac-

quisition Regulations, meaning that any public disclosure might improperly affect the bidding process.

I will assure you, Mr. Chairman, and the Committee that the FBI is committed to obtaining the best product at the lowest cost to the American people, and we do not want to prematurely disclose information which may influence bids from potential contractors.

I might turn just for a second to the issue of our human resources, which have already been mentioned by yourself, Mr. Chairman, and by Senator Leahy.

The men and women of the FBI are clearly our most valuable asset. In order to continue to recruit, hire, train, and retain quality individuals for our expanding human capital needs, we have undertaken a re-engineering of our human resource program.

We have retained the services of outside consulting firms to review business processes for selection and hiring, training and development, performance management, intelligence officer certification, retention, and career progression.

We have hired an executive search firm to identify a chief human resources officer for the FBI, an officer who has significant experience in the transformation of human resources processes in a large organization, not necessarily a governmental organization.

At the same time, we have made substantial progress in building a specialized and integrated intelligence career service comprised of intelligence analysts, language analysts, physical surveillance specialists, and special agents.

Finally, we have developed a special agent career path that will be implemented in October 2005. These career paths will take into account the background and experience of the agent in determining the agent's future career path in one of five programs: counterterrorism, counterintelligence, intelligence, cyber, or criminal. This policy will promote the FBI's interest in developing a cadre of special agents with subject matter expertise.

These are just a few of the initiatives underway to improve the FBI's human capital and to ensure that we develop a workforce that is prepared to meet the challenges of the future.

Finally, Mr. Chairman, when I last appeared before the Committee, my prepared testimony included a request for administrative subpoenas in support of our counterterrorism efforts, and I was remiss in not including that request in my oral remarks and would like to very briefly take the opportunity to do so now.

As you know, the FBI has had administrative subpoena authority for investigations of crimes from drug trafficking to health care fraud to child exploitation. And yet when it comes to terrorism investigations, the FBI has had no such authority.

We have relied on national security letters and FISA orders for business records. And although both are useful and important tools in our National security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Administrative subpoena authority would be a valuable complement to these tools and would provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and would also assist in our intelligence-gathering efforts.

I would like to stress that the administrative subpoena power would allow and provide the recipient the ability to quash the subpoena on the same grounds as the recipient of a grand jury subpoena would have the opportunity to contest such a subpoena.

Now, in closing, Mr. Chairman, I would like to address the concern expressed by some, including yourselves, that the FBI is resistant to change. One would have to admit that there are those in our organization who would adopt change more slowly than others. But I will tell you, in the 3½, almost going on 4 years that I have been with the FBI, I have witnessed the willingness of the vast majority of FBI employees to embrace change and to welcome recommendations for improvement wherever those recommendations come, whether it be Congress, the 9/11 Commission, the WMD Commission, or the Inspector General.

Since the terrorist attacks of September 11th, the pace and breadth of change within the Bureau has been significant. Occasionally I liken it to trying to change the tires on a car as it hurdles at 70 miles an hour down the road. But examples of this change are the following: We have nearly doubled the number of agents working counterterrorism investigations from 2,500 to 4,900. We have established 103 Joint Terrorism Task Forces across the country. We have embedded intelligence elements in each of our 56 field offices; they are called field intelligence groups. These did not exist prior to September 11th. We have established a Directorate of Intelligence to manage all intelligence production activities and intelligence resources. And we have collocated many of our counterterrorism personnel with counterterrorism personnel from other agencies, State and local agencies, in order to better address the global nature of the terrorist threat.

And as a result of these changes and the commitment of FBI employees to that number-one priority that you have already articulated—that is, protecting the American people from another terrorist attack—we have over the past 3½ to 4 years experienced a number of counterterrorism successes. While most of these successes remain classified or are pending matters, because of the continuing intelligence we are able to develop from them, the following are a few that you are well aware of:

The arrest and guilty plea of a group in Lackawanna, New York, pleading guilty to providing material support to al Qaeda after undergoing training in an al Qaeda in Afghanistan;

The arrest and guilty pleas of five men and one woman in Portland, Oregon, on a variety of charges, including money laundering and conspiracy to levy war against the United States, after several of them attempted to enter Afghanistan after September 11th in order to fight the American forces;

The arrest of Jose Padilla for planning activities relating to the deployment of—or undertaking a terrorist attack within the United States;

The arrest of Lyman Farris, who, after admitting to carry out surveillance and research assignments for al Qaeda, was sentenced to 20 years in prison for providing material and support.

These are just a few of those instances where, working together with others, we have been successful over the last several years. I will say that any success we have had, Mr. Chairman, is attrib-

utable to the dedicated men and women who are serving in our Federal, in our State, in our local, and in our tribal law enforcement and intelligence communities. These successes were also the result of the cooperation and assistance offered by the Muslim-American and Arab-American communities within the United States who have provided tremendous support to our efforts. These individuals and the Muslim-American and the Arab-American community share our desire to prevent any terrorist attack from occurring on our shores again. And these successes were the result of the men and women of the FBI who have embraced our changing mission, worked to enhance our intelligence capabilities, and adapted to new ways of doing business.

We still face the threat of terrorist attacks. We still face other threats that will continue to evolve. And as those threats evolve, so will the FBI as it strives to meet the challenges of the future while at the same time upholding the civil liberties we cherish.

Mr. Chairman, members of the Committee, I thank you again for the opportunity to discuss these issues concerning the transformation of the FBI, and I would be happy to answer any questions you have.

Chairman SPECTER. Thank you very much, Director Mueller, for your opening statement. We will now proceed with the Senators asking questions on our customary 5-minute round.

Let me start with the ultimate questions, Director Mueller. How secure is our homeland from a terrorist attack? Or, stated differently, what is the imminence of another terrorist attack on U.S. soil?

Director MUELLER. We are, I will say, far safer than we ere before September 11th, and that is attributable to, I believe, three factors.

The first is that we have removed in the wake of September 11th the sanctuary that al Qaeda had in Afghanistan, a sanctuary in which al Qaeda could plan, train, recruit, and coordinate, as was the case with the planning, the coordination, the recruiting for the September 11th attacks. We removed that as a sanctuary for al Qaeda to utilize.

Secondly, a number of agencies, particularly the CIA, have been successful many times over, much of that which is not recorded and in the public, many times over working with our counterparts overseas to take off the leadership of al Qaeda, to detain, incarcerate, and remove them as capable leaders in the al Qaeda network: Khalid Sheikh Mohammed, Abu Zubaida, Hambali. A number of the leadership of al Qaeda has been removed as a potential source of managerial skill, organizational skill, and that is attributable to our brothers and sisters in other agencies, but it should not be overlooked. And, finally—

Chairman SPECTER. Director Mueller—

Director MUELLER. A final point, if I can just make one more point, and I will make it brief, and that is what—

Chairman SPECTER. Okay. There are 3 minutes and 13 seconds.

Director MUELLER. I will do it in 10. The work that has been done with State and local law enforcement to work together to assure that our communities are safe. That has been tremendously important.

Chairman SPECTER. Director Mueller, we have reviewed the problems in the Virtual Case File system with $170 million being expended without any results. We are now advised that on the new Sentinel system, we are projecting a date of 2009, which is a long ways away. We saw the lack of coordination on what information we had on the FBI Phoenix report, on the Minneapolis report, on Zacarias Moussaoui, on Kuala Lumpur and the CIA. Is it realistic to be able to put all the dots on the map and all the pieces together, which needs to be done in order to prevent another attack, if we do not have the technology in place? And how can we look for a date as far away as 2009 considering all the money which has been invested and the lack of results so far?

Director MUELLER. Well, the Trilogy project had three components to it: new computers, new networks, as well as Virtual Case File. We were successful on the first parts of the Trilogy project. We have the new computers. We have the networks that support it. The Trilogy project did not at that time contemplate the database structures that we felt were necessary in the wake of September 11th to put into place to assure that counterterrorism information was in one place. We have developed—

Chairman SPECTER. Do we need that database system in order to pull all these bits of information together to prevent another attack?

Director MUELLER. We do, and we have put it together since early in 2002. We have the database structure. We have millions and millions of documents relating to counterterrorism, all of our documents relating to counterterrorism in an up-to-date, state-of-the-art, relational database structure.

The Sentinel project is due to—our hope is that we will have the contract in place by the end of this year. We expect that within a year afterwards, we will have the first deliverables. It is four stages. And the year 2009, it would take approximately 40 months—yes, approximately 40 months as we now anticipate to put into place the various components that we believe will be in the Sentinel project. And as—

Chairman SPECTER. One final question, Director Mueller, before my 5 minutes expire. There have been reports about the New York Police Department recruiting immigrants from Asia, Africa, the Pacific Islands where they have developed analyst and translator capabilities by drawing upon the immigrants familiar with languages and cultures under survey. Has the FBI undertaken a similar program?

Director MUELLER. Well, we certainly have undertaken a broad-based program to bring on board language specialists that have the full capabilities across all of the languages that we need. Some of them may well be immigrants. I will tell you, however, we have a very high standard for hiring within the FBI in terms of the clearances that are required to be obtained in order to get access to the information that we put before our translators.

But, yes, we have an active effort to recruit and bring in persons, particularly with persons who have information or capabilities in unique and very specialized dialects.

Chairman SPECTER. My red light went on in the middle of your answer, so I will now yield to Senator Leahy.

Senator LEAHY. Thank you, Mr. Chairman.

Director Mueller, there are areas where I have been critical, as others have up here, of parts of the efforts down at the Bureau. But you and your leadership team and the hard-working men and women at the Bureau deserve the constant appreciation of all Americans for all you do, and also for the sacrifices that many of you make to do it.

Now, after 9/11, the people of the FBI have put in untold overtime hours under great pressure. They have had to adjust to duties they never anticipated before that. And I compliment you and the people who work with you for doing that. And I think that it is also important that we have the oversight we do because I think it helps make everybody more effective. And that is what you and I and the Chairman and everybody else here are united in the same thing. We just want America to be safer. We want the bad guys behind bars. We want Americans to be safe.

Now, the consolidated watchlist uses, as I understand it, four risk-based handling codes. They say how law enforcement should respond when they encounter people on the list. The Inspector General report found that nearly 32,000 armed and dangerous individuals are designated for the lowest handling code. That code does not require law enforcement to notify any other law enforcement or agency or the TSC. Some of there are described as having engaged in terrorism or likely to engage in terrorism. They enter the U.S. and are a hijacker or a hostage taker of use explosives or firearms.

I understand there may be some legal requirements and there are strategic requirements, but I cannot understand why they are in such a low handling, why they are put so low. Does this put an officer who might pick them up at undue risk?

I think in my own State—and this would be the same for most rural areas—if a State trooper stops somebody at 11 o'clock at night, his back-up may be an hour or 2 hours or more away. And the person may be in one of these dangerous categories, but they are at the lowest category.

Am I missing something here?

Director MUELLER. I would have to get back to you on that, Senator. I know if the person is on the watchlist, the reason why the person is on the watchlist, there has been reason to believe that there is information or reason or evidence or intelligence to believe that the person needs to be on the watchlist. And then there are various categories, as you point out, for the handling and treatment.

The fact that the person is on the watchlist means that when that person is stopped, the Terrorism Screening Center will be alerted. And the usual practice is that when the call comes in, the Terrorism Screening Center then goes, looks at the file and talks to the agency—

Senator LEAHY. But this says they don't have to be.

Director MUELLER. Pardon?

Senator LEAHY. Those that fall in this number four category, they say the Terrorism Screening Center does not have to be notified, and yet some of them are said to be people who handle explosives—

Director MUELLER. I will have to get back to you on that, Senator.

Senator LEAHY. Well, do me a favor. If you get back to me on it, would you review the answer yourself?

Director MUELLER. Yes.

Senator LEAHY. I understand from your testimony in another case that you usually do not review these answers. This one I am very concerned about. Whether they are in rural Pennsylvania or rural Texas or Alabama or Vermont, we have very brave police officers who are out there in the middle of the night with no back-up, and when they see a name come up, they should know whether this is somebody they ought to be a little bit more nervous about.

Director MUELLER. Let me check one thing, if I could.

Yes, I will review that answer.

Senator LEAHY. Thank you. And I am disturbed by some reports from the GAO that an audit of the project, the Virtual Case File project, has been substantially delayed by the FBI. I understand that weeks go by before some meetings are scheduled. Sometimes the GAO has had to wait several months, as long as 9 months in once case, to receive documents, or the Bureau has provided wrong documents or posed other delays requiring the DOJ and the FBI attorneys to screen their documents. I know I have been told many times the FBI's answers to questions I have asked have been tied up in DOJ reviews.

DOJ has raised these problems with the Bureau. They have received assurances that things will go better. Are things going to go better?

Director MUELLER. Well, I had heard this from—it came to me from your staff several months ago, and I immediately asked persons to look into it. They met thereafter with GAO. And I believe whatever issues that were outstanding have been resolved.

Now, if you will allow me one second?

That is what I understand. Yes, I believe that is taken care of.

Senator LEAHY. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Leahy.

Senator Cornyn?

Senator CORNYN. Thank you, Mr. Chairman, and thanks, Director Mueller, for being here. You have earned all of our respect, and we appreciate your great service.

Let me just ask you about two subjects, one that I think you will regard as a fairly straightforward question. The other is not designed to be hostile but, rather, constructive and that has to do with technology that you already touched on.

I have, frankly, never understood the opposition to the use of the administrative subpoena in fighting the war on terror, as benign an instrument of law enforcement as it is to gain business records. It is already used in 335 different types of applications. Why we would deny that same tool to our law enforcement efforts when it comes to fighting the war on terror. Do you understand what the concerns are? I realize a lot of what we do here is not necessarily rational. This just seems to be totally irrational, denying that tool to the FBI, to other law enforcement in fighting the war on terror.

Director MUELLER. As I discussed in other fora as well as here, I believe it is a tool that would be exceptionally helpful, and to the

extent that we have it in 300-plus other areas, it does seem that it would be appropriate to have it in this—for use in national security investigations and terrorist investigations, and I am hopeful that this Congress will see to support it.

Senator CORNYN. Of course, the Intel Committee, in voting out its version of the PATRIOT Act, has included the administrative subpoena in its version. We did not in this Committee, but it is my hope that it can be restored on the floor and that tool can be made available.

Let me talk to you about information technology, and you have been kind enough to come by my office and talk to me about my concerns in this area. And I guess I do not want to go over old territory with regard to the Virtual Case File, but I am concerned because in 2006 it is estimated that the Federal Government will spend $65 billion on information technology. And I just want to make sure that we do not waste the taxpayers' money.

I know every taxpayer in the country would willingly send their dollars to Washington to help the FBI and other Federal agencies perform the important work that you are doing to keep us safe. But they want to make sure the money is spent wisely and efficiently.

And so would you just, in the few minutes we have remaining here, describe the steps that you have undertaken that you believe were going to result in successes in the FBI? I know the creation of the CIO has been one step, but would you describe that for us so we can have greater confidence that the FBI and other Federal Government agencies are going to be spending that money wisely?

Director MUELLER. Well, one of the things we have done is have a very competent CIO we have brought on board. We have expanded his shop. Perhaps as important, we have given the CIO's office the control over both the funds and the new projects. We have developed an enterprise architecture for the Bureau so that each new component of high-tech or information technology fits into the enterprise architecture for the Bureau.

As we have developed the Sentinel project, we have elicited support from any number of outside groups and specialists and experts. We have brought several on board ourselves to expand the CIO's office.

I can tell you as we go down this path that we will be looking for outside scrutiny and suggestions in terms of how to do it. I have a Director of Science and Technology Board that I look to with a number of people who have expertise in this arena. We have had independent assessments by outside entities such as the RAND Corporation. We deal with the Markle Foundation that focuses on these issues. We have a Strategics Guidance Council within the FBI. I have special advisers who have accomplished this type of transformation in business in the past who I call upon and get an outside view from periodically.

We want to work with the Inspector General's office as we go along so that the Inspector General can point out to us any areas in which there are flaws. We will continuously brief Congress at will. I would like nothing more than to have the process of developing this IT transparent and will take any suggestions from anybody on how to make it better.

Senator CORNYN. It sounds like you are throwing everything you can at the problem, and I congratulate you for taking it so seriously. As you working closely with the Office of Management and Budget in their efforts across—

Director MUELLER. Absolutely.

Senator CORNYN.—Government agencies to try to develop strategies to avoid these failures and to increase the likelihood of success in the future?

Director MUELLER. Absolutely, and there are some areas—and I think that the Office of Management and Budget will look at the work that has been done by our CIO shop in certain areas and say that we are leading in areas. And we in the future want to lead when it comes to information technology, as we have led in other areas. And I believe that we are building that capability.

I will tell you that I meet every week with our CIO. Myself and the Deputy sit down and go through where we are on Sentinel, where we are on the other projects. It is as important a priority as we have in order to assure that we protect the United States, particularly against terrorist attacks.

Chairman SPECTER. Thank you, Senator Cornyn.

Senator Feinstein?

Senator FEINSTEIN. Mr. Chairman, thank you.

I wanted to continue the discussion on administrative subpoenas, if I might. We discussed this privately. To the best of my knowledge, this is the first time publicly that you have asked for an administrative subpoena for intelligence purposes. You have for law enforcement purposes, but this is the first time, to the best of my knowledge, for intelligence purposes.

I voted against the intelligence bill in Committee because of the broad administrative subpoena language, and since Senator Coburn raised it, I would like to respond to it.

The administrative subpoena language in the intelligence bill is extraordinarily broad. There is no requirement for a certification of an emergency. There is no requirement for a sign-off by the DOJ, just a sign-off by the SAC. And the non-disclosure is limited.

Now, the reason that an administrative subpoena is different from the 350 other subpoenas in health and other areas is because it is not discoverable and the target essentially never knows that the Government is gathering information against them. And this can go on for years under the language in the intelligence bill. So that was one of two reasons why I voted against that bill.

I did, however, move an amendment, which I would be prepared to support, and the first part of that amendment was a certification of emergency—in other words, the rationale for needing the subpoena, the fact that it would relate to some criteria with respect to cause, that it had a sign-off by the DOJ—this could be by an AUSA—and coming to some agreement on non-disclosure.

Now, you asked for an administrative subpoena for certain specific documents that you are looking for. Let's say you go into a hotel and you say I need all of the records of everybody that is registered in this hotel. Now, in my view, you have to have cause, a rationale to do it, and that would be the certification. And the sign-off that the documents you are looking for really are relevant

would be by an AUSA, similar to what a judge might do when called on a weekend with respect to a search warrant.

Would you agree to these provisions being added to an administrative subpoena provision?

Director MUELLER. I would oppose it.

Senator FEINSTEIN. You would oppose it. You would not want any criteria at all?

Director MUELLER. I do not. Let me explain my thoughts on this, understanding your concerns.

You raised a concern that persons whose records have been subpoenaed would not find out. Well, that may well be true also in a health care or a child pornography case.

Senator FEINSTEIN. My understanding is it is all discoverable in a court of law.

Director MUELLER. If there is a case. There may well not be a case. So there may be a case on either side. But I think I am not certain that I would give a lot of weight to that particular argument.

The other argument with regard to certification of emergency—

Senator FEINSTEIN. Before you do that, let me just discuss that with you. Therefore, the Government could, under foreign intelligence, begin to collect data on people which conceivably could last for a very long time.

Director MUELLER. Relevant to a particular investigation, absolutely, in the same way we collect data now as a national security letter, absolutely. But—

Senator FEINSTEIN. But there is no criteria to show that—

Director MUELLER. Relevant to an investigation—

Senator FEINSTEIN.—it relates to an investigation.

Director MUELLER. Relevant to an investigation. And I will tell you, we had an example a couple of weeks ago in the wake of the bombings in the U.K. We had an example of a case in which an individual who was associated with the room that was believed to be the room in which the bombs were constructed, it was no longer in that area, but whenever we find out—I guess it was up in Leeds, in the wake of the July 7th bombings in the U.K. And we had an occasion in which we believe this individual had been in the United States, had gone to college in a State in the United States. The person had expertise in chemistry that would enable that person to construct these bombs. We went to the university with a national security letter. They declined to produce the documents pursuant to a national security letter. We had to, because there is a case that was aligned to it, we had to go back with a grand jury subpoena.

Now, in my mind, we should not in that circumstance have to show somebody that this was an emergency. We should have been able to have a document, an administrative subpoena that we took to the university and got those records immediately.

The other point I would make, if I could—

Senator FEINSTEIN. Let me stop you. If you will, just allow me, because I think this is really important for many of us, Mr. Chairman. Why would you—

Chairman SPECTER. Senator Feinstein, take a few more minutes here. You have been at the core of this problem in both Intelligence and on this Committee.

Senator FEINSTEIN. Thank you very much.

Why would you object to a DOJ sign-off, A, on emergency and, B, on the relationship to an investigation? I do not understand that.

Director MUELLER. Because I believe that the special agent in charge should be—

Senator FEINSTEIN. It is not going to slow anything down.

Director MUELLER. There should be a level of review, and my belief is the review should be the special agent in charge. In this particular case, it resulted in a 2-day delay.

And the other point that I would make with administrative subpoenas that is different with an NSL, and that is that the recipient of the subpoena has the right to go into court and challenge it. And so there is a process there that allows the recipient of the subpoena to go into court and challenge it before a Federal judge, and that in my mind is sufficient and adequate to assure that you will have sufficient review of that process.

Senator FEINSTEIN. Of course, with the administrative subpoena, that is not true. They do not know about it. The target does not know about it.

Director MUELLER. The third party does not, but the recipient—

Senator FEINSTEIN. But the hotel might object, using that analogy, but the target never knows.

Director MUELLER. True.

Senator FEINSTEIN. So you could do school records, you could do business records, you could do anything on anybody, and that is my concern. All I am asking for is certification of emergency, sign-off, just as you would get a judge, a police officer would pick up the phone and say, look, this has happened, I need this warrant. A judge at night would sign off on it.

See, the resistance to this makes me suspicious.

Director MUELLER. I would try to alleviate your suspicion.

I will tell you, day in and day out, we get threat information, the Internet, letters, walk-ins, about a particular person at a particular place who is going to undertake a terrorist attack. In this day and age, in order to respond to every threat, we have to go out there, we have to get records of who is in a particular hotel room, who is utilizing a particular telephone, and the need for speed is such that it makes sense to us to have the ability of the SAC to sign off in this administrative subpoena and give us the flexibility and the speed in order to get those records we need to assure ourselves that the information we may have received from the Internet or from a walk-in is erroneous and that we have done everything we can to assure that there is no further terrorist attack.

Senator FEINSTEIN. All we would be requiring would be the phone call. But it would be some oversight over the FBI within the DOJ. You do not want that. You do not want even a phone call?

Director MUELLER. I believe oversight is appropriate with assuring that the upper levels of the FBI are required to sign off on the administrative subpoena. I believe that is sufficient.

Senator FEINSTEIN. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Feinstein. Have you convinced the Director?

Senator FEINSTEIN. I beg your pardon?

Chairman SPECTER. Have you convinced the Director?

Senator FEINSTEIN. No, but then he has not convinced me either. [Laughter.]

Chairman SPECTER. Senator Sessions.

Senator SESSIONS. Senator Feinstein is such a good law enforcement supporter, I think she will be convinced before long. I am just convinced of it. This is an area that it baffles me. I agree with Senator Cornyn completely.

Director Mueller, if the Drug Enforcement Administration is investigating a drug dealer, and they are believed to have checked in at a motel, can that Drug Enforcement officer get an administrative subpoena and get the records of the motel without declaring an emergency and without having the approval of the Department of Justice?

Director MUELLER. I believe so. I have to look at the specific statute, but I believe so.

Senator SESSIONS. I believe so too. Can the IRS get people's records?

Director MUELLER. I believe that would be the case.

Senator SESSIONS. They do not have to declare an emergency to get that.

Director MUELLER. No.

Senator SESSIONS. But if an FBI agent is investigating a terrorist who may be staying at a motel and would like to verify that through motel records, they cannot get it without going to the FISA Court and getting an order that may take who knows how much time before it ever comes back to them; is that not right?

Director MUELLER. That is one of the avenues. We do have the NSL avenue, but that is one of the avenues.

Senator SESSIONS. I just think this is unbelievable that we would provide all kinds of health care document that can be produced by the health care inspectors and other people that collect these documents and we cannot do it for our National security. Of course people collect the documents and the FBI maintains a file on it, but it does mean that they are going to produce that to the world or prosecute somebody who is innocent. I just really am concerned about that. I think this is a good thing.

Would you think that if a FBI special agent in charge, which is a fairly august position at least in the eyes of those who work for that agent in charge, maybe send a copy of it to the U.S. Attorney or something if that would make people feel better, but to me we ought to have at least the powers that we have in other agencies of Government to investigate terrorism. Would you comment on that in general?

Director MUELLER. I would agree. I do believe if you have it in 300 plus other circumstances, including child pornography, IRS, and certain areas of the DEA, it would be not only appropriate but an important device for us to have as we address not just terrorism investigations, but counterintelligence investigation and investigation in which other countries, other people are seeking to steal our

secrets and provide it either to groups outside the United States or other countries outside the United States.

Senator SESSIONS. I would just share this thought. Historically, public documents outside the control of an individual—you have been a long time prosecutor. You have handled these things for many years. You are a professionals professional. You serve Republican and Democratic administrations. You have been United States Attorney in a high position in the Department of Justice. You have personally prosecuted lots and lots of cases. You understand what it is like in a courtroom.

So my question is essentially, has it not always been the legal principle that with regard to documents outside your control, not the records you have in your house or in your desk at your office, but where you sign a motel receipt or a phone receipt, you do not have the same expectation of privacy in that document as you do something that is within your own personal sphere of control; is that correct?

Director MUELLER. That is accurate and the Supreme Court has so held. In fact, it was Sandra Day O'Connor in a case—I cannot remember the name off my head—that held that.

Senator SESSIONS. So whenever you sign in at a motel, the clerk knows your name and what you filled out. Anybody that works at that motel you have an expectation has access to that document or else they would not have asked you to fill it out. It does not have the same degree of secrecy that you would if it were in a document maintained in your home.

Director MUELLER. Correct.

Senator SESSIONS. So that is why we have always done that, used to in the past, motel records, even telephone records were turned over by these entities whenever you asked for them.

Director MUELLER. Grand jury subpoena generally, standard is relevance.

Senator SESSIONS. But in the old days, when Dragnet and Jack Webb and all were investigating crimes, they would just go down to the motel and the guy would give it to them, right? Normally.

Director MUELLER. Normally, yes, way back when.

Senator SESSIONS. Then they started being afraid they would be sued or something, so they will not give any records. They want a subpoena, and an administrative subpoena will allow for that and maintain a record of it. If they do not want to turn it over, they can file a motion to quash.

Just one more thing if you would. I think the Nation has been watching the case involving Natalie Holloway in Aruba.

Director MUELLER. Yes, sir.

Senator SESSIONS. She is a resident of my State. We have been concerned about that. I understand that the Aruban authorities in recent days have been more open with the FBI. I think you have personally made some effort on it. What can you tell us about the status of that?

Director MUELLER. Originally I did talk to the Attorney General down there, and we had a number of agents that were helping out, assisting in the initial stages of the investigation. We currently are offering expertise to the Aruban authorities to the extent that we can provide it, and in the last couple of days I believe we have been

in discussions where we are offering and providing expertise to the Aruban authorities in hopes of having a break in that case.

Senator SESSIONS. I certainly hope so. I have been told by the Prime Minister that he welcomes any assistance, so if there is not full cooperation, I hope you would let me know so we could approach that with him.

Director MUELLER. Yes, sir.

Senator SESSIONS. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Sessions.

We now have Chairman's call. Senator Feingold was here earlier but left, and Senator Durbin has been here longer. But we passed you by, Senator Feingold, so the tie goes to you. You are next in line.

Senator FEINGOLD. Thank you, Mr. Chairman.

Thank you, Director, for not only being here today but for the time you spent with me in my office recently which was very helpful.

I am pleased that there was a good exchange before I got here with Senator Feinstein about these administrative subpoenas. We talked about it at some length, and I do hope that you will continue to consider alternative ways that we can get at these problems which you explained very well to me in my office, but I really hope we do not have to have such broad powers used in order to get at these emergency situations.

I would like to talk to you about the bill that the Senate Judiciary Committee unanimously reported out of Committee last week reauthorizing the USA PATRIOT Act and making some changes to some of its most controversial provisions. As I stated last week, the compromise bill made some meaningful improvements but did not address everything that I believe needs to be revised. One provision that I would have liked to have seen in the bill is an ascertainment requirement for roving taps under the Foreign Intelligence Surveillance Act, just as there is now an ascertainment requirement in the criminal law for roving taps. It is a simple concept. It ensures, when the order itself does not designate the phone or the computer to be tapped, that the investigator actually has a sufficient basis for turning on a wiretap of a particular phone or a computer. It just ensures that innocent people's phone and computer conversations are not intercepted.

Would you have an objection to including an ascertainment requirement for FISA roving taps?

Director MUELLER. I would have to look at that, Senator. I will tell you one of the things that is a challenge is this day and age is the swiftness with which some discard communications devices and replace them. I would certainly look at and consider any language that you would propose, but I expect to balance it against our need to move efficiently from communications device to communications device without always having to go back to the FISA Court on a daily or hourly basis. So I would have to look at it.

Senator FEINGOLD. I understand the need for that kind of balancing. I guess I would just like you to speculate on how this works, how an agent makes the decision of which phone or computer to tap. If you do not somehow ascertain that the target is

using the phone or the computer, how do you decide which phone or computer to tap?

Director MUELLER. First of all there has to be the belief that the person is a agent of a foreign power or a terrorist so there has to be some initial threshold finding before you get to the device that is being used, and then the application would have some description of the device or types of devices or where they are being used or how they are being used in order for the court to be able to articulate an appropriate order to the facility that was providing the service. So inherent in that process is some degree of specification.

Senator FEINGOLD. This is the whole point of ascertainment. You do have a target out there. You have somebody you are concerned about. But how do you connect that person to the particular phone or computer without an ascertainment requirement?

Director MUELLER. It depends on the circumstances. I would have to look at your—

Senator FEINGOLD. You have indicated a willingness to look at it. I think this is a gap that we need to change something about this in order to protect innocent people, and I hope we can work together on that.

I would like to get your response to some testimony we heard at a PATRIOT Act hearing a few months ago. One of the witnesses at that hearing was Suzanne Spaulding, who has spent a good portion of her career working on intelligence issues at the CIA on two different commissions examining issues relating to terrorism and weapons of mass destruction, and in Congress where she had the privilege or working for our Chairman and on the Intelligence Committees.

She explained why we have to be particularly careful in the oversight of intelligence investigation, and I want to read what she said. She said: "Intelligence operations by necessity are often wide ranging rather than specifically focused, creating a greater likelihood that they will include information about ordinary law-abiding citizens. They are conducted in secret, which means abuses and mistakes may never be uncovered, and they lack safeguards against abuse that are present in the criminal context, where inappropriate behavior by the Government could jeopardize a prosecution."

She continued: "Because the safeguards against overreaching or abuse are weaker in intelligence operations than they are in criminal investigations, powers granted for intelligence investigation should be no broader or more inclusive than is absolutely necessary to meet the national security imperative and should be accomplished by rigorous oversight by Congress, and where appropriate, by the courts."

Do you agree with the statement and sentiments that I just read?

Director MUELLER. She said an awful lot in that statement. There are certain aspects that I would agree with. I do believe that one has to be careful in establishing, for instance, an intelligence directorate or a national security service, that one has an objective for the collection of intelligence. I do believe that one of the reasons both the 9/11 Commission as well as the WMD Commission believe that the growth of a domestic intelligence capability in the United

States should be in the FBI is because we have a lengthy detailed training with regard to the controls on our activity, whether it come from the Constitution, whether it come from statutes, whether it come from the AG guidelines.

I do believe that one of the reasons that it is important for the FBI to undertake this capability is that I think we have a way of looking at sets of circumstances that is fact driven and is consistent with the Constitution, its applicable statutes and the AG guidelines.

By the same token, I do believe that in order to address the threats of today and tomorrow in terrorism, weapons of mass destruction, there has to be a growth and some capabilities along the lines of administrative subpoenas to allow us to have access to the information that will alert us to the threats against the United States, with appropriate Congressional oversight.

One of the things that I do believe is important for us and others is to see what you have done but not put impediments to action. In other words, in my mind, adding a test or issuing administrative subpoenas are impediments to swift action, where you can look after the fact and see if it was appropriate. And in my mind, as you build an intelligence capability, as you look at oversight, there needs to be oversight in the institution, in the Department of Justice, but the oversight should not inhibit the swift reaction to a set of circumstances that you just do not know where it is going to go and you have to act quickly.

Senator FEINGOLD. Thank you, Mr. Director.

Chairman SPECTER. Thank you, Senator Feingold.

Senator Durbin.

Senator DURBIN. Thank you very much, Mr. Chairman.

Thank you, Director Mueller, for being here. I continue to have the greatest faith in you. I think you were an excellent choice by this administration. You have served our Nation well, and I would say the same for all the men and women who work at your Agency. We are fortunate as Americans to have people with your dedication to the common good and the protection of America. Thank you for your service.

You have been very open with me. There have been times when we have had discussions where you were candid about your misfortunes and disappointments, and things that we had hoped would turn out better. So please take whatever I ask in that context. I respect you very much for your public service.

Let me go if I can to the underlying—I have two questions, and I will state them both though they are unrelated, because I will run out of time otherwise.

The first is this. We have had several colleagues talk about the PATRIOT Act. I voted for the PATRIOT Act. It was a strong bipartisan vote for passage of it, and I commend the Chairman and other members of the Committee. Our proposed revisions of the PATRIOT Act passed 18 to nothing on a strong bipartisan roll call, and that is exactly the way it should be. I think we found the right balance between security and liberty in what we have come up with to revise the PATRIOT Act.

If you will listen to the questions of my colleagues and mine, you will understand there is still an underlying concern that maybe we

have gone too far in some specific areas of the PATRIOT Act, gone too far in compromising our basic rights and liberties as individual citizens.

The reason I raised that—we are not going to resolve that today, not likely we will at any time in the near future. But the basis for the PATRIOT Act is to give the Government the authority it needs to collect enough information, intelligence, to protect us from terrorism, and crime for that matter, but protect us from terrorism.

What troubles me is as we debate about how wide we are going to open the top of this funnel to collect information, once collected, that information passes through a very narrow chute when it comes to the analysis of the information, the collection, the analysis of that information and the sharing of that information, and it is at its narrowest point in your Agency at this moment. I think it is reflected in the fact first of the information technology problems which beset this Agency for a decade or more. According to Judge Webster, you are facing an obsolete system today at the FBI. It is clear from all analysis that it will take as long as 3½ years from now to complete the Sentinel system which is the modernization of your information technology, which means from start to finish, 9/11 to completion of the system, 8 years, 8 years.

Secondly, the Inspector General talks about the backlog of collected counterintelligence and counterterrorism audio, that we still have more than one-fourth of that that goes unevaluated, unreviewed. Even as we collect more and more information we still do not have the people to review it to determine what is important there to keep us safe. 10 years to coordinate our fingerprint collection from start to finish when the Federal Government said to the then Immigration Naturalization Service and the FBI, can you collect the same sets of fingerprints so you can share this information? Maybe at the end of 10 years they will have been able to accomplish that simple task. Then of course the information that will come out in this hearing, that about one out of five of your intelligence analysts plan to leave within the next 5 years.

So when you put all this together, my basic question to you is one that my former Congressional colleague and Commissioner of 9/11, Mr. Hamilton, is going to raise later on. If it is going to take us another 3½ years to get all this together, can we afford to wait? Can we say that that is an acceptable timeline? Is there anything you can do or we can do to speed this up and to make certain that intelligence gathering analysis and collection is done in a more timely fashion?

The second question, totally unrelated, goes to the administration's interrogation techniques. These have been extremely controversial. The idea that we would change our approach in interrogating prisoners and detainees in the war on terrorism has been the subject of a lot of debate, dissension from people like Secretary of State Colin Powell, JAG lawyers, an amendment pending on the floor yesterday from Senator McCain, Senator Graham and Senator Warner about whether or not we ought to be more explicit in saying the United States will not engage in cruel, inhuman and degrading treatment of prisoners.

Your FBI agents have been some of the most outspoken critics of this administration's interrogation techniques, saying in memos

that we have received that have been declassified, that first, torture is ineffective. A person in pain will say anything to escape the pain. Secondly, that the techniques that are being employed go too far. Some of your FBI officials have said they are not permitted by the U.S. Constitution. Others have said that they are harsh techniques that do not produce good intelligence.

My question to you is this. I want to commend the FBI for standing up for American values. I think you are recognized as the Agency that probably has been the premiere agency in effective interrogation techniques. What has been your reaction to the interrogation techniques of this administration, the critique of your agents, and to your knowledge, have the Defense Department's interrogation changed because of FBI oversight and observations of excesses?

Director MUELLER. Let me start on the delay that it is going to take in various areas to get where we want to be. I do not see an endpoint. Information technology has to grow month by month, year by year. Sentinel now is going to be in four stages. We have 100 different programs, different systems, many of which are obsolete. You have to do a triage on those systems to put into place new systems that will give you the same information but in different ways. One of the things that people do not recognize, that it was a huge advance for us to have everybody with the most modern computers, to have the networks in place, the modern networks, and to have the database structures in place that will enable us to share that information.

So I see Sentinel as one piece of a process where it is going to be in four stages. We get returns 12 months from December, hopefully. I will say "hopefully" given my experiences. And then several months or a year afterwards the next iteration of it. We tend to look at this as one project, look at it as a whole, but there are other things that will be happening at the same time, and it is an iterative process. What we have done in my mind is put into place the capability to manage this process as a large corporation, modern corporation would. When it comes to human resources, what we need to do is put into place the same capabilities that a large corporation would have in order to bring people on board to recruit them, to hire them, to train them and to retain them. We are putting in place the, redoing the infrastructure to put in place a modern human capital capability that will enable us to do this down the road.

I see putting into place these building blocks that will enable us in these other areas, besides just investigation, besides just intelligence gathering, but enable us to conduct these two activities much more effectively and efficiently than we have done in the past. But it is a continuous iterative process. So we will have returns far before 2009 or 2011 or 2015, but you get to 2009, the process and the capability still has to be there to build.

With regard to the question in terms of the interrogation techniques, I have not been—

Senator DURBIN. If I could ask you one last follow-up on the—

Chairman SPECTER. Senator Durbin, you are three-quarter minutes over. How much more time will you need?

Senator DURBIN. I was living by the Feinstein rule, but the Durbin rule is a much shorter one, so whatever you can say I would appreciate.

Chairman SPECTER. You are past the Feinstein rule, Senator Durbin, but my question pending is how much more time do you need?

Senator DURBIN. Just if he could answer the last question.

Chairman SPECTER. Okay, fine. Go ahead, Director Mueller.

Director MUELLER. Our agents have followed the protocols that have established in the Bureau over a period of time. To the extent that we have had information brought to our attention, where we believe that matters should be taken up by other authorities, we have provided that information to the Department of Defense the follow up on.

Senator DURBIN. I am sorry. I did not understand your response.

Director MUELLER. Where we have information relating to standards of interrogation that we did not believe may be appropriate, we have taken those pieces of information and provided them to the DOD to review and to address.

Senator DURBIN. If I had time, I would ask you whether they had changed their interrogation techniques as a result.

Chairman SPECTER. Senator Durbin, do you have another question? Go ahead.

Senator DURBIN. That is my last question.

Director MUELLER. I do believe they have, but I am not privy myself to the changes and the developments in that regard, but I believe they have.

Chairman SPECTER. Senator Durbin, you did not have another question. Director Mueller just had another answer.

Senator Kohl.

Senator KOHL. Thank you very much, Mr. Chairman.

Director Mueller, there was a story in the New York Times the other day about how fearful Londoners are to ride the subway. My question is, why should citizens here in our country feel any safer in the subways of America? What can you tell the American people about our law enforcement officers today and the system that we have going that would get them to feel that law enforcement here is better than it was in London, and that they should not be as fearful as Londoners are today?

Director MUELLER. Allow me to say I happened to be on a prescheduled trip in London last week, and I can tell you the Londoners go about their business the next day. They have been through this before. The fact that there was a second wave certainly would cause some concern, I will tell you that the Londoners are back in those subways. The ridership was not down much at all, and if it was down, it was down a day and then was back up a day afterwards.

We have, I believe, in the United States, together with Department of Homeland Security, the State and local law enforcement authorities, through our joint terrorism task forces, through our relationships, through understanding the threats to our communities including our subways, have worked together to do what we can to protect the subways, to do what we can to protect the trains, and there probably is more that can be done. The fact of the matter is,

you can never protect it 100 percent. You can never protect it 100 percent. And so you want to minimize, reduce those risks. We are doing everything we can to minimize, reduce those risks.

Throughout the United States we are sitting side by side with State and local law enforcement, understanding what is in the community, the threats in the community, and when we see a threat in the community, we have moved quickly I believe to address those threats either by prosecuting the individuals on material support where it is appropriate, prosecuting the individuals for other criminal offenses where it is appropriate, or in other case where the person is here illegally, deporting the person where it is appropriate.

Senator KOHL. You feel that people in our country have legitimate reasons to feel safer because of the measures that we take, that you take with your Department, and Homeland Security takes, then perhaps people in London?

Director MUELLER. I think that it is just not Homeland Security, it is not just the FBI, it is other Federal agencies, it is State and local law enforcement, and it is our intelligence community operatives overseas that have had as much or an effect in terms of disabling al Qaeda as any entity in the United States, as I pointed out before. Detaining and removing from the battlefield the leaders of al Qaeda were done by our sister agencies, and they have done a fantastic job and that has made us safer. I always say it has made us safer, not safe.

Senator KOHL. Speaking about al Qaeda, how would you assess the level of threat that al Qaeda poses today? Is it closer to what the administration officials have repeatedly been telling the American public, or closer to the assessment of other terrorism and intelligence experts who believe that they are still today coordinating attacks as the London attack?

Director MUELLER. I think most people would agree that there are a number of instances in the past where individuals who have an ideological compatibility with the violent extremism articulated by bin Laden have come together to undertake attacks. The extent of the direction from afar is different depending on the attacks. It may be financial support. It may be information and capabilities in manufacturing devices. But you have to look at each incident to determine to what extent there was support from outside the place in which the incident occurred, and to what extent that can be tied to a particular person who is known to be in the inner circle of al Qaeda, and that is difficult to do.

I will say, as I was saying before, I think we are a lot safer, certainly a lot safer than we were before September 11th, but the fact of the matter is, while we are a lot safer, you cannot 100 percent guarantee there will not be another terrorist attack.

Senator KOHL. What makes it so terribly difficult for us to capture Osama bin Laden?

Director MUELLER. I would hesitate to speculate that. That probably should be directed to others in the intelligence community, because I am somewhat familiar with the terrain and the difficulty in operating in the terrain where he is believed to be. I am somewhat familiar with the difficulties in identifying with specificity where he is, but I am certainly no expert in that.

Senator KOHL. Thank you.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Kohl.

Senator Biden.

Senator BIDEN. Thank you very much, Mr. Chairman. I apologize, I had to be in Delaware this morning at the State Fair to speak to the agricultural community, and I apologize for being late, Director.

Let me begin by thanking you. I think you are doing a heck of a job, and I think you are doing a heck of a job under very, very difficult circumstance, and all of us so-called policymakers and administrations and Congress, we all like finding somebody else to blame for some of our problems, and your Agency has been I think the target of some criticism I do not think it has deserved.

I would like to make one broad statement and then ask you to respond to a few specifics. It is sort of like we have had a perfect storm occurring here. We had a decision made based upon—and I am not asking you to comment—but a decision, right or wrong, to end the COPS program, drastically cut the aid to local law enforcement for no hiring and for a lot of other things. We were providing over $2.4 billion in local law enforcement aid. Now we are down to $167 million. The aid that goes through Homeland Security, none of that is allowed to be used for hiring personnel, and it is less than targeted.

You have had enormous additional responsibility placed upon you in the counterterrorism area, enormous. You have justifiably and understandably had to tell local law enforcement, overstating it to make a point, we do not do bank robberies or interstate car theft any more; you guys are on your own. Violent crime task forces have had to be curtailed. It is not a criticism, it is an observation. I do not know how you could do it with the number of agents you have. My recollection—and I am sure they are in my notes here—I do not recall them exactly, but the total increase in the number of agents is de minimis since 9/11, and at the same time we are getting reports—and I am going to ask you to comment on this—from the Counterterrorism Center, John Brennan, and many others because all of us have been dealing with this in other capacities beyond this issue, that a greater threat is homegrown terrorism, not importation. I do not know if that is true. I am going to ask you whether you agree with that.

The end result of all of this is, it seems to me—and I know you are in a tough spot; I do not know what your answer would be. I hope it would be candid or you would just demur, but not tell me something that is not—and that is, I think you need 1,000 more agents. I am not being facetious. I think you need 1,000 more agents. I think we have to reconstitute the Violent Crime Task Force. I think you have to be able to walk and chew gum at the same time. I think we cannot—not the you are leaving it hanging, but you are not able to assist locals like you were before.

With all your intelligence work, and pray God—I see the Co-Chairman of the 9/11 Commission is here—pray God these fixes will be successful. But it is more likely to be some local cop coming from the Dunkin Donuts Shop, going behind a super mall in my State or yours, that detects a guy climbing out of a dumpster, who

has just put Sarin gas in the ventilation system. It is not going to be a guy with night vision goggles, and you are not going to be able to all the time have the intelligence to anticipate where this is going to occur.

And I add one last factor. I think it is close to politically—if there is such a phrase—criminal for us to not have provided additional security for rail. We are nowhere near safer, notwithstanding what the great Director says. All I ask you to do is leave here, go get in the train that the Chairman and I get on as it takes out Union Station, go to the back window, look out the window. Tell me how many cops you see. Tell me whether you see any protection of the switching devices. Tell me if you see a single camera. Tell me whether you see anything, anything, anything. More people visit that facility than any other facility in Washington.

This morning there were more people sitting in an aluminum tube underneath the tunnels of New York City than in 7 full 747s, virtually no ventilation I say to the Chairman of the Commission, no lighting, no escape of any consequence, tunnels built in 1917. Go through the Baltimore tunnel built in 1869, no ventilation, no lighting, no escape under the harbor. This is criminal.

Now, it is none of your responsibility, Director, but if you add all these things up, it seems to me you need more resources. Are you able to do what you think you need to do with the roughly—what do you have now, about 14,000?

Director MUELLER. We are up to 12,500 I think.

Senator BIDEN. 12,500.

Director MUELLER. Approximately.

Senator BIDEN. Is that enough?

Director MUELLER. Well, we have had to prioritize. We have been working, for instance, with the Inspector General's Office to determine where there have been—since we have reprioritized and made our first priority counterterrorism, making certain that we follow every counterterrorism lead, there are areas in which we have not been as active as we have been in the past. I believe that the studies will show that there has been a picking up of the slack by the DEA in drug cases, as well as State and local law enforcement. We still will, in isolated circumstances, do bank robberies, where they are armed bank robberies, where we can add something. But where we do not add something to the table, we have had to prioritize and focus our efforts, and I think we are doing a fairly good job on it.

There is one area in which I believe we will have to look at in the future, given what I believe the IG report may come out with, and that is when it comes to smaller white-collar criminal cases, with the Enron cases, with the Qwest cases, with all of those cases we have had to put substantial resources on the larger white-collar criminal cases, focusing on those, and the smaller white-collar criminal cases which we have done in the past, we are not doing so much of, and that is an area where I think there is a gap that we will have to look to.

We have in front of Congress the 2006 budget, where we are receiving additional resources. My expectation is I will ask for additional resources in 2007. I will tell you that we have had to reprioritize and we will continue to have to do that, but that is not all together bad either, because we should use our unique capabili-

ties where they are necessary, and not replicate the capabilities of others because we like doing it.

Senator BIDEN. May I have 30 seconds more, Mr. Chairman, to make a brief comment?

Chairman SPECTER. Go ahead, Senator Biden.

Senator BIDEN. My dad used to say, if everything is equally important to you, nothing is important to you. You are being asked to prioritize and you are put in a tough spot. I would like to throw you in the briar patch. I believe it is absolutely irresponsible for us not to be increasing substantially the FBI, substantially the aid for transit in this country, and substantially local law enforcement. And for the President to tell me there is a priority on a tax cut, tell me there is a priority on anything else, I find irresponsible. If you cannot walk your streets, if you cannot be safe, if you cannot provide for a better shot at dealing with terror, then it seems to me none of your other liberties from education to highways makes any sense.

I thank you, Mr. Chairman.

I am going to try very hard to throw you in the briar patch.

Chairman SPECTER. Thank you, Senator Biden.

Director Mueller, just a couple of more questions before turning to the second panel with respect to your comments on the PATRIOT Act. We have made a fair number of changes to accommodate what the FBI have said after the Specter-Feinstein bill was introduced. We have eliminated the reporting on FISA, on the pen register because you thought that was troublesome. We have had sunsets on some of the provisions and not on other provisions.

As to the roving wiretap, we have inserted a requirement to have some idea as to who is the subject, so you just do not have John Doe, and it is consistent with your prior representations that even when a target's identity is unknown, you must have significant information about the person before initiating a roving wiretap.

We have omitted the mail cover, but you did not even ask for the mail cover, which is an expansion of authority, which is in the Intelligence Committee. That is correct, is it not, Director Mueller, that you did not ask for the mail cover?

Director MUELLER. Did not. That does not mean, however, that we would not like to at least have it. We did not request it, but in reviewing that bill, it is something that would be beneficial because it would enable us to have more authority over obtaining the mail cover information that we currently have, but I did not ask for it, you are right, Mr. Chairman.

Chairman SPECTER. Director Mueller, we would have to guess about what you wanted if we were to include things you did not ask for. And then on the scale of what is really necessary, we obviously weigh pretty critically what you have not asked for as not being as important as what you have asked for, pretty fundamental analysis.

With respect to section 215, we have inserted language on relevancy which meets the grand jury standards. You had commented that you do not have to show probable cause to get a grand jury subpoena, which you are exactly right. The grand jury has a proceeding which seeks to establish probable cause. On the requirements of section 215, we have said that there ought to be a state-

ment of facts showing "reasonable grounds to believe that the records or other things sought are relevant to an authorized investigation."

The PATRIOT Act currently has a relevancy standard, but does not have any elaboration as to what that means. We have a number of prosecutors on the Committee who dealt with probable cause, and it is a lower standard. It is a standard, as I have said on RT enterprises. So what we have tried to do is to have a balance. As you well know, the PATRIOT Act has been challenged from both the right and the left, a lot of concern about civil liberties, a lot of concern about terrorism, and our Committee has tried to strike a balance.

We had a remarkable result in getting all 18 Committee Members to agree, including the one Senator on a 99–1 vote in 2001, who did not favor it, and I am advised this morning that the two leaders are what we call shopping unanimous consent request, because it appears that the bill which the Senate Committee turned out has met with almost universal approbation.

Let me give you one last chance to register whatever complaints you have as to what you think ought to be changed from the bill which passed out of our Committee.

Director MUELLER. Let me thank you for all the work that has been done on the PATRIOT Act. This Committee and Congress as a whole, I saw some time ago a fairly broad gap, and I think that has been closed. It is very narrow at this point. There is one area in which—

Chairman SPECTER. Very narrow at this point, a very narrow gap at this point?

Director MUELLER. Very narrow at this point, very narrow.

Chairman SPECTER. Good.

Director MUELLER. There is one area under 215 where we would agree with the relevance standard, but there is an additional phrase in there—and I would have to get back to you on this—that ties it to an agent of a foreign power, and the relevance standard, given our—well, the relevance standard which we think is appropriate, should not be limited by a further showing of relating to an agent of a foreign power. I would have to get you the specific write-up on that phraseology, but that is the one piece that I think is still outstanding that we have some concern about. If you allow me just for a second to check.

There is one other problem that I—

Chairman SPECTER. The provisions that you may be referring to, Director Mueller, is the language pertains to a foreign power or an agent of a foreign power relevant to the activities of a suspected agent of a foreign power who was subject of such authorized investigation, or pertaining to an individual in contact with or known to a suspected agent of a foreign power.

Director MUELLER. In our minds it should be relevant to an investigation as opposed to having to identify a particular person.

Chairman SPECTER. If that is the only gap we have, provide additional information because we will be going to conference with the House and we want to very, very carefully consider any request you have.

Director MUELLER. Thank you very much. Thank you for that opportunity. We will do so. I appreciate it.

Chairman SPECTER. Director Mueller, thank you for two hours plus. It is a long session, but you saw a lot of interest here by the Members. We know how busy you are, so when we have you at the witness table, we like to ask you lots of questions.

There is one more that I told you I was going to ask you, and that is about the Journalist Privilege Statute. Deputy Attorney General Comey did not come in when we had that hearing last Wednesday, and we had given you notice in advance that this would be an opportunity for the administration to state whatever objections the administration has to that proposed legislation. So now is the time.

Director MUELLER. If I could, I have not been involved in discussions there. I know Deputy Attorney General Comey filed a statement in opposition to the legislation, and I am sure as a representative of the Department of Justice and the administration, that statement should stand as the policy, or the views, I should say, of the Department of Justice on that legislation.

Senator LEAHY. Mr. Chairman, if I could?

Chairman SPECTER. Senator Leahy.

Senator LEAHY. I was far from satisfied with Mr. Comey's statement. I think part of it looked like it was prepared prior to some of the changes made and some of the legislation. I am very disappointed.

This is not directed at you, Director Mueller, and your answer is the only one you can give I think under the circumstances, but I was very disappointed that Mr. Comey did not testify. I think this whole question of a shield law, however you describe it, is an important one. It is one that one way or the other the Congress is going to wrestle with. I would hope that we have Mr. Comey up here to testify, or the Attorney General, to testify on this because it is not fair to put you in the position to have to. I think at some point we are going to have to because there is going to be legislation that will be coming forward on a shield law, and a lot of us would like direction more than a out-of-date statement, with almost like a note saying, oh, by the way, I cannot show up. That is not at you. I am just saying that we have to have some.

Director MUELLER. I am not certain what iterations the legislation has gone through the committees. I was alerted to the fact that I would be asked the question, and a statement would stand as the position of the Department. I will say that one of the concerns that I will voice here, I think is a very valid concern, is that one would not want to have a mini-trial every time you need information from somebody associated with some form of the media, whether it be television or the newsprint or what-have-you. So in looking over it briefly and not having spent any time on it, that is something that jumped out at me as a concern that we would have or I would have in terms of conducting investigations.

But I preface this, or I guess add to it the fact that I have not had an opportunity to review the legislation itself. I have had an opportunity to look at the statement of Mr. Comey, and that is something that stuck out at me as something that I think we would be validly concerned about.

Chairman SPECTER. Thank you very much, Director Mueller.

Director MUELLER. Thank you.

[The prepared statement of Mr. Mueller appears as a submission for the record.]

Chairman SPECTER. We will turn now to our second panel. Inspector General Glenn Fine of the Department of Justice; former Congressman Lee Hamilton; former FBI/CIA Director William Webster; and Program Manager, John Russack, of the Information Sharing Environment, Director of National Intelligence.

Thank you for joining us gentleman, and thank you very much for your patience.

Our first witness is Inspector General Glenn Fine, has an outstanding academic background, magna cum laude from Harvard, Rhodes scholar, BA and MA degrees from Oxford, law degree from Harvard. Prior to joining the Department of Justice's Office of Inspector General, Mr. Fine practices as an attorney specializing in labor and employment law. In 1995 he joined the Department of Justice and served in varying positions, including Special Counsel to the Inspector General, Director of OIG Special Investigations, and Acting Inspector General.

Thank you for joining us, Mr. Fine, and as you know, we have 5-minute rounds, and then 5-minute rounds of questioning. Thank you for being here, and we look forward to your testimony.

STATEMENT OF GLENN A. FINE, INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. FINE. Mr. Chairman, Senator Leahy, Members of the Committee, thank you for inviting me to testify regarding the oversight work of the Office of the Inspector General within the FBI.

In my written statement I provide a summary of the findings of several recent OIG reports, such as reviews of FBI intelligence analysts, FBI information technology, the Terrorist Screening Center, and intelligence information related to the September 11th attacks. I also describe several ongoing OIG reviews in the FBI of interest to the Committee, such as the FBI's compliance with the Attorney General's investigative guidelines, the FBI's handling of the Brandon Mayfield case, and the FBI's observations of alleged mistreatment of detainees at military detention facilities.

In my testimony this morning I would like to provide observations on the FBI's transformation and key challenges it faces, and briefly summarize the findings of an OIG report released today that examines the FBI's foreign language translation program.

The FBI is undergoing significant changes since the September 11th terrorist attacks. Despite shortcomings we have found in some FBI programs, I believe that Director Mueller is moving the FBI in the right direction, but there are areas in the FBI in need of significant improvement. The first is the urgent need to upgrade the FBI's information technology. Without adequate information technology, FBI employees will not be able to perform their jobs as fully and effectively as they should.

Second, our reviews have found that the FBI is affected by high turnover and key positions at headquarters and in field offices. For example, in the past, rapid turnover in IT positions hurt the FBI's

ability to manage its information technology modernization projects.

A third critical challenge facing the FBI is its need to effectively and efficiently share intelligence and law enforcement information, both within the FBI and with its law enforcement and intelligence partners.

Fourth, the FBI must value to a greater degree FBI staff with technical skills. While the FBI's culture is changing, more needs to be done to support the work of intelligence analysts, scientists, linguists and other staff who are critical to meeting the FBI's changing mission.

Fifth, the FBI previously exhibited an insular attitude with an aversion to oversight. In the last several years the FBI has opened itself to outside scrutiny from the OIG as well as other groups. While not everyone in the FBI has welcomed such change, I believe the Director, senior FBI leadership, and many FBI employees recognize the benefits of this oversight.

I would like to now turn to the OIG report regarding the FBI's foreign language translation program. In July 2004 the OIG completed an audit which found that the FBI's collection of counterterrorism and counterintelligence audio material had outpaced its translation capabilities. The audit also found that the FBI had difficulty in filling its need for additional linguists.

Because of the importance of these issues, the OIG conducted a follow-up review this year to assess the progress of the FBI's translation program. Our follow-up review concluded that the FBI has taken important steps to address recommendations from our previous report, and has made progress in improving its translation program. However, we found that key deficiencies remain, including a continuing backlog of unreviewed counterterrorism and counterintelligence materials. For example, the FBI estimated that its counterterrorism audio backlog was 4,086 hours as of April 2004. In this follow-up review we found that the counterterrorism audio backlog had doubled to 8,354 hours. Although that is a small percentage of total counterterrorism audio collections, the FBI has no assurance that these materials do not contain important counterterrorism information unless they are reviewed and translated.

We also attempted to determine the priority of the counterterrorism material that was not reviewed. We found that none of the counterterrorism audio backlog was in the highest of the FBI's five priority levels, that almost all of the backlog was in cases designated in the second and third highest priority levels.

With respect to counterintelligence collections, the amount of unreviewed material is much larger and has also increased since our previous report.

Our review also found that a continuing issue for the FBI is the time it takes to hire contract linguists. According to even the FBI's statistics, the average time to hire a FBI contract linguist has increased from 13 months to 14 months.

In sum, our follow-up review found that the FBI has made progress in improving the operations of its translation program, but key deficiencies remain.

While I believe the FBI is moving in the right direction, it needs to make further progress in its foreign language program as well as in other critical areas. To assist in these challenges the FBI will continue to conduct reviews in these important FBI programs.

That concludes my statement and I would be pleased to answer any questions.

[The prepared statement of Mr. Fine appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Inspector General Fine.

I will not turn to former Congressman Lee Hamilton, a colleague on the Hill with both Senator Leahy and myself for many years. He has served some 34 years in the Congress before undertaking activities with the Woodrow Wilson International Center for Scholars. Congressman Hamilton's resume is so long, it is difficult not to get lost in it. While a member of the House of Representatives for some 34 years, he was Chairman of the Permanent Select Committee on Intelligence, Chair of the Joint Economic Committee, Chair of the Joint Committee on the Organization of Congress, and without objection, we will put a full copy of his resume into the record because it is very long.

He was Co-Chair with former Senator Howard Baker on the Baker-Hamilton Commission to investigate security lapses at Los Alamos, and his most recent post was Vice Chairman of the 9/11 Commission which did such an extraordinary job in leading to the revisions of our National intelligence structure.

A graduate of DePauw University, Indiana University School of Law, attended the Goethe University in Frankfurt, Germany. While this is the last line, it may be the most important, former high school and college basketball star and a member of the Indiana Basketball Hall of Fame, which is no mean accomplishment.

Thank you for joining us, Congressman Hamilton, and we look forward to your testimony.

STATEMENT OF LEE H. HAMILTON, PRESIDENT AND DIRECTOR, WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS, WASHINGTON, D.C.

Mr. HAMILTON. Thank you, Chairman Specter. Of course the reason I was elected 34 times was that I was in the Basketball Hall of Fame. I think that was the chief reason.

[Laughter.]

Mr. HAMILTON. Chairman Specter and Senator Leahy, I am delighted to be with you this morning.

I think the best thing for me to do is start with my conclusion, and that is simply to say that on the 9/11 Commission we said that our recommendation was to leave counterterrorism intelligence collection in the United States with the FBI, and that that assessment requires that the FBI make an all-out effort to institutionalize change, and if it does that, it can do the job.

We still hold to that assessment. We believe that Director Mueller is making a very strong effort to effect change. We believe the obstacles are immense. We applaud the progress that he has made. We urge him to forge ahead, and we want to give him our support so that he can get the job done. We want to try to be help-

ful and constructive. We believe that the FBI has been reforming itself for 4 years, and everybody recognizes, as does this Committee for sure, there are still significant deficiencies. I will mention then in just a moment. It is fair, however, to ask the FBI how long is it going to take to make these reforms? Director Mueller's timeframe for effecting reform at the FBI is not, should not be infinite.

The United States has not been attacked at home since 9/11, but we all understand the threat of terrorism is very real. It is also true that the threat to reform is real. The threat is inertia and complacency. We need to maintain a sense of urgency to push the reform forward as quickly as possible. I believe this Committee has a very important job to do with its expertise in providing oversight to the Director, and I am pleased to see you had this hearing this morning.

Let me identify very quickly for you the areas that I think need real emphasis with regard to the FBI's progress, and that you need to watch carefully. One of course, as you have heard about already, that is the question of analysis. The FBI must have a strong analytical capability to drive and to focus its work. The traditional division between the agent and the non-agent—and we all know that in the past being an agent puts you in a very superior position in the FBI. The FBI, however, now, with its new function needs to have the best possible analysis. The collection of intelligence is not worthy very much if it is not adequately translated into realistic threat assignments. The FBI did not perform that job prior to 9/11.

Doing the job well has to be a priority. You cannot decide what actions to take, you cannot decide what priorities to make, if you cannot assess the nature of the threat. So the Bureau needs to become a premiere agency for analysis. In order to do that it has to give analytical capability the attention and respect that it deserves. There have been some problems, as have been cited for this Committee, with regard to attrition rate for analysts and many other things.

A second point is information sharing. The biggest single impediment to all source analysis is the resistance to sharing information. We found of course that sharing the right information with the right people in a timely fashion is critical, and we again, and again, in the report stress the necessity of sharing intelligence.

Now, there are a number of barriers to that, and so breaking down those barriers has to be a very high priority. You have to motive institutions and you have to motivate individuals to share information. Congress created this position of the Program Manager—he is sitting with us this morning—for Counterterrorism Information, sharing across the Federal Government and with State and local agencies, and also as appropriate with the private sector. But if you are going to be effective in sharing information, you have to have leadership at the top.

The success of information sharing needs the personal attention and the support of the Director of the FBI. It needs the personal support and direction of the Director of National Intelligence, and it needs the personal attention and support of the President of the United States. Only the President can lead a Government-wide effort to bring national security institutions into the information rev-

olution, and that is absolutely critical if you are going to have the kind of information and the kind of analysis of the information that is necessary to stop terrorism.

Two or three other matters and I will conclude. FBI management. Obviously there has to be greater stability in management. Mr. Chairman, you cited the figures early on. Another point is the relationship between the National Security Service and the Director of National Intelligence and the FBI. The FBI is shifting to an all together different paradigm to prevent counterterrorism, and it has to be institutionalized. The WMD Commission recommended the National Security Service. That is a good recommendation because it makes permanent some of the reforms that we have been talking about.

I see my time is concluding. Let me just say very quickly that the FBI has to have strong relations with the CIA. The relationship between the two has to be seamless. We must not tolerate any more failures to share databases on terrorists between agencies. The FBI relationship with foreign and domestic intelligence services is critical and has to be strengthened, and setting priorities for State and local government is important as well.

Often I have encountered sheriffs and policemen who say to me, in this whole effort of counterterrorism, what am I looking for? What am I trying to get from the FBI? What does the FBI want from me? The idea is that the FBI of course has to build a reciprocal relationship.

Finally, let me say the whole question of civil liberties—you have been talking about that very much this morning—but I believe it is important for the Director of the FBI, Mr. Mueller, for Mr. Negroponte and others in leadership to say loudly and clearly by word and deed on law enforcement, terrorism prevention and also on the protection of civil liberties, and that becomes an immensely important part of the so-called war on terror.

I have gone over things very, very quickly, Mr. Chairman. I will be glad to elaborate on them, and of course I ask that my statement be submitted into the record.

Chairman SPECTER. Without objection, Congressman Hamilton, your full statement will be made a part of the record.

[The prepared statement of Mr. Hamilton appears as a submission for the record.]

Chairman SPECTER. We now turn to Judge William Webster, who has had a storied career, a Federal Judge in the District Court in Missouri, Court of Appeals Judge for the Eighth Circuit, Director of the FBI, Director of the CIA. We will put into the record his very long list of other public accomplishments.

Amherst College graduate, law degree from Washington University. A frequent visitor to the Judiciary Committee over the year. Thank you for joining us, Judge Webster, and the floor is yours.

STATEMENT OF WILLIAM H. WEBSTER, PARTNER, MILBANK, TWEED, HADLEY & McCLOY, LLP, WASHINGTON, D.C.

Mr. WEBSTER. Thank you, Chairman Specter, Senator Leahy. Thank you for the privilege of appearing before you this morning to discuss generally the role of the FBI in collecting, assessing, data mining and sharing intelligence of interest to many agencies,

Federal, State and local, who have been waging the battle against terrorism, especially since the tragedy of 9/11 almost 4 years ago.

While the emphasis is on an examination of progress made since 9/11, I think, if you will permit me, some reminders of an earlier period are in order in order to add some context to what has become the FBI's response to terrorism.

I took office as Director of the Federal Bureau of Investigation in February 1978 in the wake of the investigations which led to the Church and Pike Committee reports. When I called on Vice President Mondale as a new Director, he presented me with copies of both reports and admonished me to read them carefully. These reports contained strong recommendations against the CIA engaging in activities inside the United States, and discouraged the FBI from engaging in operational activities abroad. The predominant restrictions related to "need to know," and that was the hallmark.

In the 14 years that I served first as the Director of the FBI and then as Director of Central Intelligence, the guidance that we received from the Department of Justice and our own legal counsel was strongly influenced by those two Congressional documents. A reasonable shorthand would be: Stay away from each other. Beware of using evidence developed through intelligence sources in criminal investigation, and on it went.

But of course there were exceptions, and important cooperation did occur in the worldwide struggle against terrorism. For example, in 1987 a notorious terrorist, Fawaz Younis, was located in Cyprus after he had left his Sudanese sanctuary. The CIA managed to lure him into open waters, where a U.S. Naval vessel was waiting just over the horizon. The arrest was effected by FBI special agents, and he was brought to the United States where he was tried and convicted. There are other examples, but of course they were largely overseas, but I mention the fact that it is not true that the FBI and the CIA could not, when called upon to do so, work closely and successfully together.

In 1987 when I was Director of Central Intelligence, I signed a memorandum of understanding with the Director of the FBI, following the unfortunate Edward Howard investigation in which the CIA agreed to notify the FBI promptly whenever one of its employees became a suspect on national security issues. This is a recurring theme, getting the two organizations together in a timely way in order to do good work.

The adoption of the PATRIOT Act following the 9/11 tragedy, shifted the emphasis to "need to share." It was like a large ship changing course against the tides of Church and Pike. Getting the word out and understood was doable, but not an easy task. Moreover, the archaic condition of the Bureau's electronic case management system, designed during the Church-Pike Committee days, did not lend itself readily to tasking from other agencies of the intelligence community. Efforts to patch what is now a 14-year-old mainframe has been both expensive and frustrating. I put this right at the top of problems affecting information sharing by the FBI with other agencies.

When I chaired a special commission to examine the internal security provisions of the FBI in the wake of the arrest and conviction of Robert Hanssen in 2001, we filed four classified appendices

to our report relating to these computer deficiencies. I believe that more than patchwork, however expensive, is absolutely required so that the FBI can fulfill its mandate of sharing the vast amounts of intelligence which can be mined from its stored data.

Although I have seen reports to the contrary, I believe it is unfair to attribute problems and information sharing to cultural attitudes. I believe they are more rightly attributed to the understandings that flowed from the Church and Pike Committee reports and were underscored and supported by departmental guidance and Congressional opposition to domestic intelligence sharing. In my 9 years at the FBI I found the men and women ready to respond to new directions that did not embroil them in unfair charges or put their careers at risk. The various joint projects, such as counterterrorist centers, brought the CIA and the FBI closer together in a common cause.

Still, in my view, "need to share" is not a total substitute for "need to know." Sources and methods must be protected and honored if law enforcement and intelligence agencies are to be effective in recruiting and utilizing information obtained at great risk from such sources. There also continues to exist the problem of the third agency rule, under which the FBI or the CIA receives sensitive information from the intelligence agency of another country on condition that it not be shared outside the agency to whom it is presented.

I see that my time is expiring if not expired, and I will try to be fast about this, but I am currently serving as Vice Chairman of the Advisory Council on Homeland Security, an organization established by President Bush shortly after the 9/11 tragedy, and with the creation of the Department of Homeland Security, we have been directed to work closely with the Secretary of Homeland Security, one of the challenges to make important sensitive information available to the Department of Homeland Security, and at the same time honor the "need to know" principle. There are as many as 100,000 first responder agencies, police departments, fire departments and so forth, who are most likely, as pointed out, to be first on scene, and may also be best suited to prevent a terrorist incident if they have the needed information.

Homeland Security is entitled to and does receive intelligence from the CIA, the FBI and other members of the intelligence community. First responders rarely need to know the sources of the information or the methods by which the information was obtained. I believe it is sufficient to supply these agencies promptly with finished intelligence, which sets forth the information without disclosing sources or methods. There may be more exceptions, but this should certainly be the basic principle if sensitive sources are to be protected.

In 1978 when I took office the three top priorities of the FBI were organized crime, white-collar crime and foreign counterintelligence, a considerable shift in gears from the days of stolen cars and bank robberies. I added terrorism to that list in 1980.

We have been experiencing approximately 100 terrorist incidents a year, certainly not of the dimension of the attack on the World Trade Center, but life-threatening, lethal and a danger to our society. Within the FBI we focused on getting there before the bomb

went off. Prevention and interdiction obviously depended upon much better intelligence than we had had in the past, and we worked on this, developed our sources, worked effective undercover operations, and acted preemptorially when appropriate. As I moved to the CIA in 1987, we were down to 5 or 6 terrorist events. In the year following, there were none. I attribute this to highly skilled, dedicated professional law enforcement, and especially to better intelligence, along with cooperation from friendly agencies in Canada and other parts of the world.

We have made very substantial progress in coming to grips with even larger terrorist activities and plotting in the past few years, but intelligence is the key, as every speaker before me has said this morning. Without it, the terrorist is likely to succeed in his terrorist activity, leaving it to law enforcement to track him down and prosecute him. Prevention requires intelligence.

In summary, I believe the FBI has significantly transformed itself to meet the current threats. It does probably need to improve its analytical capability which historically has been under developing. Translators are badly needed to keep up with processing signals intelligence, documents and other important information. But the biggest challenge in my view is to confront in a rational way the consequences of an archaic electronic data system that preceded the PATRIOT Act and would be considered obsolete by any modern enterprise. It needs a search engine that can be navigated with much greater speed and with more precision in locating those dots that were not found when they were needed.

The FBI deserves a great deal of credit for many forensic improvements, DNA, the computerization of fingerprints, psychological profiling and other scientific techniques, and these efforts should be supported and properly funded, but it makes no sense to have the best trained special agents I the world if they are not properly equipped and guided by the best available information. Sir William Stephenson, the famous "man called Intrepid," once wrote about the importance of gathering intelligence and managing the process, and he concluded that in the integrity of that guardianship lies the hope of free people to endure and prevail.

If you will permit me another moment, and with all respect, when we talk about guardianship there is also the matter of oversight. The special commission on 9/11 strongly recommended that the Congress streamlined its oversight procedures, and in my view, this has not yet happened. It is my understanding that there are some 88 Congressional committees that claim oversight responsibility in the Department of Homeland Security alone, and this needs to be addressed.

Finally, we now have a new organization in the intelligence community and a new leader. While the 200-page Act covers many of the issues, the key authorities of the Director of National Intelligence were not as expressly granted as I would have liked, but I believe that Director Negroponte will assert them fully as needed. Of paramount importance is his responsibility to insist upon the level of cooperation and sharing among the members of the intelligence community that I believe the President and Congress—

Chairman SPECTER. Judge Webster, how much longer would you need?

Mr. WEBSTER. I am finishing my sentence and that is it.

That I believe the President and Congress intended in this reorganization, and that it be done with appropriate protection of sources and methods so essential to our National security. And as Congressman Hamilton, and in preserving at the same time the civil rights that are so important to us.

Thank you.

[The prepared statement of Mr. Webster appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Judge Webster.

Our final witness on this panel is Mr. John Russack, recently designated by the President to be Program Manager, responsible for terrorism information sharing pursuant to Intelligence Reform and Terrorism Prevention Act.

Mr. Russack has a long, distinguished career in the Navy, Navy Captain, commanded the Aegis cruiser, has worked in the CIA as Director of Operations, has worked with the CIA's Nonproliferation Center, and I note is a graduate of the University of Kansas. Are you a native Kansan, Mr. Russack?

Mr. RUSSACK. No, sir, I am not.

Chairman SPECTER. Too bad for you.

[Laughter.]

Senator LEAHY. In case you did not realize, the Chairman is.

Chairman SPECTER. And also ROTC graduate, but Air Force. If it had stuck to ROTC I might have had a distinguished career by this time. But I note your Kansas affiliation and I could not resist the temptation to ask you.

Thank you for joining us, and we look forward to your testimony.

STATEMENT OF JOHN A. RUSSACKS, PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT, DIRECTOR OF NATIONAL INTELLIGENCE, WASHINGTON, D.C.

Mr. RUSSACK. Thank you, sir. Thank you for the opportunity to be here and appear before you and Senator Leahy and to join this panel.

As you noted, I was appointed by the President in April to be the Program Manger for the Counterterrorism Information Sharing Environment. I am responsible for planning and overseeing the implementation of that environment, to make improvements on the already existing environment, to work on policies, procedures, guidelines, rules and standards that pertain to the environment, and then I am to support, monitor and assess the implementation, and in fact, report progress on the implementation to the Congress, to you, sir, to Senator Leahy, and to the President of the United States.

Let me first of all say that the mandate for the Program Manager extends across the Federal Government, and then up and down from the Federal Government to State, local, tribal and the private sector. So the environment is not just Federal, it is all-encompassing. We are sharing information better than we ever have. However, the present environment at best is flawed. We need to share it even better than we do today, and that is my mandate. I am a volunteer for this job. I care very deeply about information sharing and in fact about the national security of my country. I will

be assisted in accomplishing this task by a very small staff of approximately 25 people, most of whom will come from detailees from other parts of our Government. I will probably hire about 5 or 6 people, and the remaining 20 will come, as I said, as detailees.

I will also be assisted in the job by an Information Sharing Council. As you recall, Executive Order 13356, which was signed by the President last August, started work on the information sharing environment. In fact, I led the mission team responsible for Section 5, which was a plan for the information sharing environment. We divided in half, a technical side and a mission side. So I am familiar with the issue, and in fact the impediments to information sharing.

I was required by law to issue to the Congress and to the President a report on the 15th of June. I did that. The basic content of that report was a summary of the impediments to information sharing. And to sum that report up, sir, I would say that the impediments are not the flow of electrons. In fact, technology is an enabler to information sharing. Most of the impediments that we have today to information sharing have to do with roles, missions, responsibilities that sometimes overlap, occasionally they conflict. They are training, they are fostering changes in the way we do business, and I think that we can achieve over the next 2 years—I have been appointed to this job for 2 years, and at the end of 2 years I make a recommendation to the Congress and to the President on how the information sharing environment is at the end of 2 years, and what the future of the present position I have been appointed to will be.

But I think we can make dramatic improvements in information sharing. I will also say that most of the low-hanging fruit has been plucked. What is left to be done is really hard, and I welcome your oversight, and I look forward to reporting to you and to Senator Leahy, and the rest of the Committee on our progress as we make information sharing better than it presently is today.

Thank you, sir.

[The prepared statement of Mr. Russack appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Mr. Russack.

Mr. Fine, you have published reports going into some detail as to the failures on the FBI, noting five missed opportunities to prevent the September 11th attacks, lack of effective analysis, failure to use the Foreign Intelligence Surveillance Act. Beyond the role of being a critic, you get very, very deeply involved in all of these issues. Have you made any affirmative suggestions to the Bureau as to how to solve these problems? As I listen to the plight of the Bureau, there are lots of difficulties, and a constant theme is things are improving but not enough. But from your vantage point as Inspector General, it seems to me you would have the capacity to—maybe it is beyond your purview, but your purview could be changed—to make suggestions to the FBI as to how they ought to correct these problems. Have you worked that angle of the issues?

Mr. FINE. Yes, Mr. Chairman, we absolutely do that. One of our missions is obviously to look backwards and find out what went wrong and to assess the current state of affairs within the FBI, and we have found key deficiencies, but we do believe it is one of our

most important missions to also provide recommendations to them on how to improve the operations of these very important programs.

In each of our reports we make recommendations to the FBI. In our information technology report we made a series of recommendations on how to better oversee the acquisition of information technology, in our intelligence analyst reports as well. So in each of our reports we provide recommendations to them and we follow up on them to see whether they are implementing our recommendations. In many cases they say they have or will take corrective action. With healthy skepticism we try and go back and see whether they do, and in fact, that was the genesis of our follow-up report on the foreign language translation. We did our report in July 2004. We made a series of recommendations, and we wanted to see whether they had actually implemented those recommendations. They had some. They have more progress to go on others as well.

Chairman SPECTER. Congressman Hamilton, your leadership on the 9/11 Commission, along with the Chairman was certainly exemplary, and you are pursuing the Government, notwithstanding—you filed your report. I do not know that your Commission is over. And you have articulated a sense of urgency which I think is right on the button. What are the plans for the 9/11 Commission to raise hell with the intelligence agencies to see that they follow your advice?

Mr. HAMILTON. Well, the Commission, Senator, of course if out of business. It was a statutory commission and our time expired last year. We did move ahead, Tom Kean and I, and raised some money privately for a public discourse project in order to try to push forward some of the recommendations not adopted.

Chairman SPECTER. But are you not still in the wings, fronting the Federal agencies?

Mr. HAMILTON. We are. We took very seriously the recommendations we made, and we want to push them forward. We have been really pleased really that many of them have been adopted by the President and by the Congress, but we feel the number is still dangling out there, including the one that Judge Webster mentioned a moment ago on Congress. Congress has not done what it ought to do with regard to getting its oversight function more robust, and that is a serious problem I think, and there are other recommendations we are going to push forward. We are pushing forward the idea that Homeland Security funds need to be distributed on a risk assessment basis and not on the basis of politics. We are pushing forward the idea that a part of the radial spectrum should be dedicated to first responders. That is a no-brainer from my standpoint. I cannot understand why it takes so long to get it done.

We are pushing forward the idea that much, much more emphasis has to be put on the weapons of mass destruction coming into the hands of terrorists. We have a lot of things we are pushing on, but none really any more important than what we are talking about this morning, trying to get the FBI to make the kind of changes that are necessary.

I sit here this morning and I listen to all of these things that are being said, and I think they are almost all on the mark, and yet

it sounds to me very much like business as usual. And business as usual is not satisfactory.

Chairman SPECTER. How do we change that?

Mr. HAMILTON. Maybe London will change it. Maybe Madrid changes it. I do not know. But I think there does need to be a much greater sense of urgency. When I hear about some of these reforms not coming into effect till 2009, I say to myself, you are just giving the terrorist activities an opening, and the risk goes up for the American people the longer you extend these deadlines, the more time you take to make these changes.

I agree with everything that has been said about the remarkable that Director Mueller has made, but he needs a lot of support from many of us in order to get this job done with greater sense of urgency.

Chairman SPECTER. I am going to go over a little on time. I want to ask a question of both Judge Webster and Mr. Russack and the hour is growing late, so I will try to be brief.

Judge Webster, you have the unique background of having been the Director of both the FBI and the CIA, and you cite the Fawaz Younis case which is a fascinating case. I recall that. About 1983—I would have to go back and look at the record—but I believe that I posed in one of the hearings where you testified an idea that I had about kidnaping terrorists. There was a U.S. Supreme Court decision in 1886, where a man accused of fraud in Illinois went to Peru, and the Supreme Court was very blunt in identifying his return to Illinois to face criminal charges as having been kidnaped. Fawaz Younis was not technically kidnaped because he was on the Mediterranean, but you cite that as an illustration of cooperation between the FBI and the CIA.

What insights do you have as a result of your being Director of both of those agencies to find some way to have them do a better job in talking to each other, or do you think that problem has now been solved?

Mr. WEBSTER. Well, I recited at perhaps too great length the consequences of the Church-Pike Committee reports that drove it in the other direction, and the sudden change that occurred with the PATRIOT Act. I have watched and believe that the two organizations sincerely desire to work together. They have different missions, like the nature of the intelligence that they gather and whether it can be used in a criminal court under the Brady rule if it is offered in evidence and they have to tell where it came from.

So some of these problems still need to be addressed, and Congress can play a role in that. But I think the toughest problem—and I know that I am making more of it than I should in terms of the time I take—is getting the FBI to the point where it is capable of supplying the vast amount of information that the CIA and other agencies legitimately want to know. Their old mainframe was designed to chase criminals, and it was organized on an investigative structure that only permitted you to ask one or two questions in order to get answers. It is really archaic, and although Congress has generously given many millions of dollars to fix it, I do not believe it is going to be fixed until people are brought in who understand it. I would say get Bill Gates and tell him to take 6 months and help us solve our problem.

In the past I the construct of this, we were anxious to get in the computers. I started the computerization of fingerprints 100 years ago, but we tried to do it too much with our own people, thinking we could do anything that we set our minds to do, and we did not identify and bring in the kind of expertise that was necessary. It is badly needed now. It is indispensable now. When I hear talk about providing more agents, that is great, and it has a great deal of appeal to be able to tell constituents that I got 1,000 more agents for the FBI, but there is no sex appeal in getting a new computer. But my point I tried to make in my remarks was you have to—if you are going to have the best trained people in the world, you have to equip them appropriately rather just add to their numbers, and that is where we need it.

Chairman SPECTER. I have another question or two for you, Judge Webster, and for Mr. Russack. But I am going to yield now to Senator Leahy.

Senator LEAHY. I was struck by the comments made by several on oversight and other things. Congressman Hamilton is an old friend, whom I respect greatly, and I would note on one thing, we talk about the number of committees that might have oversight, there has been precious little oversight. Except for Senator Specter and a couple of others, there really has not been. There have been many requests for oversight and for years after 9/11 we were told that it might be embarrassing to the administration to have real oversight, so we should not have any. And a complacent and compliant Congress went along with that.

We do not look at some of these problems that Inspector General Fine has pointed out, and he incidentally, is one of the finest public servants I have ever known, and has done great, great service to all of us, to the FBI and to the Department of Justice, to the Congress, and we do not take advantage of that adequately. We do not follow up on a number of things. We can spend 4 months in the Senate talking about nuclear options, and the American public is not fooled that we are not talking about somebody setting off a nuclear bomb, but we are talking arcane procedural matters within the Senate.

We can certainly ramp up and go fast and tell the Schiavo family, irrespective of the tragedy of their family, irrespective of the fact that courts have done that, by golly, the Congress can step in and we can make the decision for them because it happens to be the headline that day. We have fallen down on the job. The 9/11 Commission was helpful. I do not know how many people were paying attention to it.

The question I have of Mr. Russack is—and I am trying to do this without going into classified areas so I will be somewhat general—we talk about the weaknesses of threat assessments. I do not find an awful lot of products that look across the intelligence community and all the various aspects as you have, the nature, range, likelihood and target of long-term terrorist threats. One of the greatest terrorist events in the United States was Oklahoma City, and I like to think that a white, American, former military, devout religious person and all that, that that is not a fair assessment to jump up, and let us hope it is unique. But I find when I talk to State and local authorities, who are oftentimes the ones who are

going to see these people first, that there is confusion about the roles of the FBI, DHS, the Terrorist Threat Integration Center, how that works.

Are there impediments here? Can we improve the area of threat assessments? I realize we do a lot of the symbolism things. We have a 90-year-old women going through the airport being told to take her shoes off, and has to explain with some desperation the nurse at the nursing home usually does that, she cannot do it. That may make us feel safer, but are there impediments to improvement in the area of threat assessments?

Mr. RUSSACK. Senator I think there are some impediments. Some of what you ask me goes well beyond the realm of my job as the Program Manager for Information Sharing, but what I see from my vantage point is a real effort on the part of—let us just take NCTC, the National Counterterrorism Center, as an example. I see a real concerted effort on the part of organizations like NCTC to do a better job in threat assessments.

Even if you have a better threat assessment, you also bring up the problem of impediments to sharing that information, and you cited an example from State and local government. I think there are impediments to sharing. I think what we will do on the Program Manager's staff for information sharing and then the Information Sharing Council is try and codify or make better, develop the business rules for information sharing, and provide State and local government a clearer point of contact. In other words, make unmurky the presently at least somewhat murky waters. Try and make it clearer what they need to worry about, and in fact, try and share information, all forms of information with them, you know, keeping a balance, as Judge Webster said, between need to share and need to protect sources and methods.

I think we can share more and still protect sources and methods, and at the same time, give State, local, tribal and the private sector better information with which not only to act upon and hopefully prevent terrorist activities, but also in the case of the private sector, State, local and tribal, to also protect what they need to protect.

Senator LEAHY. Thank you. I appreciate that.

We have gone over time. I want to thank both Lee Hamilton and Bill Webster. They have given enormous pro bono time, and I appreciate this. It is sort of like you leave Government and you think you have left, but nobody lets you leave. I appreciate the time you spend on that. And within Government, superb people like Mr. Russack and Mr. Fine. I think a lot of us forget how fortunate we are in this country, people not only in Government, but people who have left Government and are willing to come back.

Mr. HAMILTON. Senator, I thank you for that. I want to emphasize here the importance of this job of Program Manager. The whole thrust of the 9/11 Commission report was you got to share information better. The impediments are not hard to find. The impediments are stovepiping within agencies. They do not want to share information across agencies. The impediments are so much emphasis on the need to know that you ignore the need to share. Bill Webster is absolutely correct, you have to get the right balance in there, but for years and years in the intelligence community, the

whole emphasis was on need to know, need to know, need to know. That excluded a lot of people, and it brought about in fairly direct terms, 9/11. We simply did not—

Senator LEAHY. Look at the people from Oklahoma who were out—

Mr. HAMILTON. We simply did not share the information we needed. Okay. Now you come along with a new structure, and the place where it all comes together is in Mr. Russack's position. He is the Program Manager. He is the fellow that has to see that we get all of this information shared. And if you do not get that information shared across agencies, if you do not get the information shared vertically within the FBI, as well as horizontally across various intelligence agencies, you are not going to have the most effective means of fighting terrorism.

So the Program Manager's position has to be empowered. He has to have the resources. He has to have the people. He has to have the political support in order to get the job done.

Senator LEAHY. I agree. That is why my first question was to Mr. Russack. We are counting on people like him pulling these things together. I think of those people who are trained to be pilots, and the area FBI call in with their concerns to headquarters and being basically told, no, there is nothing for you to worry about, and we do not want you to keep bothering us. Go about, I guess, catching bank robbers or car thieves or something, and of course, these are the pilots that flew airplanes in 9/11.

Inspector General Fine, if I might, I have one more question. I keep going to this linguist area. I have the frustration of many of us, how few Americans actually learn other languages or can speak other languages and how it hampers us in dealing now with some very, very serious problems. You conducted an investigation, you did the audit of the translation program. I have that from July of 2004. But you conducted an investigation into the allegations of lax security and possible espionage as made by a former contract linguist. And you made some recommendations regrading security in the translation program. How do you feel about the security of the program? How has the FBI responded to the recommendations you have made?

Mr. FINE. I think they have generally responded well. We followed up on that and tried to provide an assessment of where they are now in our follow-up report. They do now have written guidelines for risk assessments and how to judge whether there are risks involved with the hiring of certain contractors. There were no written guidelines in the past. They now have instituted a procedure whereby the supervisors assign who is going to be translating which materials, rather than the linguists themselves, which created problems in that case. They are trying to train the linguists better, and they are also providing better tracking of which linguists translate which material so there can be an audit trail.

So they have made some changes. Their policy manuals are not complete, and they are still making further changes, but I think they are generally receptive to it.

I do believe in the importance of oversight, the importance of Congressional oversight and Inspector General oversight, and we see that when we come back and try and follow up, that often

spurs them into a sense of urgency to get it done, and I think that is what is happening here. I do think they are receptive to it, but needs more that should happen.

Senator LEAHY. Thank you very much.

Thank you, Mr. Chairman. If I have any other questions, I will submit them later.

Chairman SPECTER. Thank you, Senator Leahy, for your service in 3 hours plus, Ranking Member. Where are all of our colleagues now?

Senator LEAHY. I think what they are doing is frantically trying to rearrange the schedule now that the Republican leadership is overriding you and saying we want to have the Roberts hearing in August. So I am hoping you are able to override the override.

Chairman SPECTER. If we go back to that, there will be no more questions for anybody except Judge Roberts.

[Laughter.]

Chairman SPECTER. Mr. Russack, you said you have a 2-year appointment and at the end of 2 years your office expires?

Mr. RUSSACK. Yes, sir. The Intelligence Reform and Terrorism Prevention Act required that the President designate me, and it says in the law that I shall be designated for a period of 2 years. In fact, there is a caveat in there that says—

Chairman SPECTER. Does the whole office sunset at 2 years?

Mr. RUSSACK. Excuse me, sir?

Chairman SPECTER. Does the whole office sunset? FBI Director Mueller should have heard about a 2-year sunset for the entire office. He would have been appalled.

Mr. RUSSACK. Yes, it does.

Chairman SPECTER. He does not want—

Mr. RUSSACK. As a matter of fact, there is a caveat that says it could actually expire sooner if I do not do a good job, so I am committed to do a very good job.

Chairman SPECTER. Are you doing a good job? To ask you a leading question?

Mr. RUSSACK. I think the answer to that question is we are just getting started.

Chairman SPECTER. I asked you the leading question for a purpose. I am advised by counsel that you do not have any employees.

Mr. RUSSACK. Well, I have one. I have one and I have two contractors, so there are four of us right now. So we are making progress, Mr. Chairman. In fact—

Chairman SPECTER. Progress?

Mr. RUSSACK. Yes, sir.

Chairman SPECTER. Sufficient progress, Congressman Hamilton?

Mr. HAMILTON. It is not even close.

Chairman SPECTER. Your office has been in existence for a year, Mr. Russack, and to have one employee and two contractors, that sounds very nebulous to me.

Mr. RUSSACK. Mr. Chairman, the office has not been in existence for a year. In fact, I was designated in April, and in June it was decided that I would work for the President through the DNI. So we have—

Chairman SPECTER. Was the Program Manager for Information Sharing, was that position created a year ago?

Mr. RUSSACK. It was created with a law, and the law said that—

Chairman SPECTER. When was the law signed?

Mr. RUSSACK. I am not exactly sure. I know it was signed in 2004.

Chairman SPECTER. Could it have been a year ago?

Mr. HAMILTON. It was December. It was December last year.

Chairman SPECTER. Is that sufficient progress, Inspector General? We are going to take a vote here, Mr. Russack.

[Laughter.]

Chairman SPECTER. You may lose your office sooner.

[Laughter.]

Chairman SPECTER. How do we get the sense of urgency? I am overriding the question, Mr. Fine. I am withdrawing the question.

How do we get the sense of urgency? Congressman Hamilton, do you—that is right on the head. Now, how do you do it? If you have some ideas and bring them to this Committee, we can have oversight, except that I am not sure Judge Webster likes it because we are one of 70 some committees exercising oversight, and they all have long hearings. This is a short hearing for oversight.

[Laughter.]

Chairman SPECTER. How do we get the sense of urgency, Congressman Hamilton?

Mr. HAMILTON. I think oversight is a very tough problem for the Congress. I do not know of any way to do it, Senator, except the way you are doing it. You have got a marvelous staff in back of you, and your job, it seems to me, is to be both a critic and a partner with regard to the FBI. You want to help them as much as you can, but at the same time you want to point out areas where you think better performance can be made. One of those things is to convey that sense of urgency.

All of us on the 9/11 Commission are very worried about this. There was a real sense of urgency in this country after 9/11. And we have been very fortunate not to have had an attack here. But so many things intervene, that we tend to lose it. I think one of the responsibilities of a Congressional Committee that exercises oversight is to try to impress upon the Director and his staff that sense of urgency.

Chairman SPECTER. Judge Webster, you are currently the Vice Chairman of the Homeland Security Advisory Council. So are you still on the payroll?

Mr. WEBSTER. No, I am not.

[Laughter.]

Chairman SPECTER. No payroll for that, but at least you have an official position. Unlike the 9/11 Commission, your Advisory Council is in business.

Mr. WEBSTER. We are in business.

Chairman SPECTER. Are you raising hell with the Homeland Security folks to give them a sense of urgency?

Mr. WEBSTER. We are trying to do that, and we are actively inspecting sites to see what progress has been made in beefing up the various agencies. We have undertaken task forces, one of which addresses the whole issue of public source information and how it could be marshaled to help our joint effort. It is a Committee of

some very good people, I might say, and they have taken on individual task force assignments.

Chairman SPECTER. Mr. Russack, we want to help you. If I were to write a scathing letter, whom would I address it to to give you some help?

Mr. RUSSACK. Well, first of all, before I answer that question, let me just tell you, sir, that we have been working hard on this, even though we have a very small staff.

Chairman SPECTER. Do not need any help?

Mr. RUSSACK. Yes, sir. I mean I am not saying id o not need any help. In fact, what we just did is write a letter to the deputies of the departments and agencies within the Federal Government and define the positions that we are trying to fill, and I can assure you that there is a sense of urgency to get those positions filled. Yes, I do need help.

As Congressman Hamilton said, I accept your criticism. I would like to point out that we are very small, we are working very hard. Filling the positions that we have defined is going to be critically important, and I think you write your letter, since I work for the President through the DNI, to the Director of National Intelligence, and express your concerns.

But I can also tell you that the Director of National Intelligence cares very deeply about this office and he is committed to helping. So I accept your help in addition, sir.

Chairman SPECTER. I know the Director, and I am going to write to him.

They just brought me another bottle of Gatorade which is indispensable to sustain me, so we can go another 40 minutes.

[Laughter.]

Chairman SPECTER. Thank you, gentleman, for coming in, and thank you for your patience in waiting through two preliminary hours, and we are more than an hour into this panel. You bring a great deal of experience and a great deal of expertise to these issues.

And this Committee is going to be undertaking oversight on a very extensive basis, and it is not too gratifying sometimes because the same problems seem to recur, and the sense of urgency really is hard to transmit.

You, Mr. Russack, have a really critical position by the way the title sounds, and your background in the Navy and CIA and DCI, you are really in a position to do something. So consider yourself a quasi-adjunct to the Judiciary Committee, and we are going to write to the Director, and let us know if you need more help.

Mr. RUSSACK. I will, sir.

Chairman SPECTER. Thank you all. That concludes our hearing.

[Whereupon, at 12:40 p.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

January 3, 2006

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed please find responses to questions posed to FBI Director Robert S. Mueller III, following Director Mueller's appearance before the Committee on July 27, 2005. The subject of the Committee's hearing was oversight of the Federal Bureau of Investigation.

We hope that this information is helpful to you. If we may be of additional assistance in connection with this or any other matter, we trust that you will not hesitate to call upon us.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Responses of the Federal Bureau of Investigation Based Upon the July 27, 2005 Hearing Before the Senate Committee on the Judiciary Regarding FBI Oversight

Questions Posed by Senator Specter

1. Larry Johnson, a former counter-terrorism official at the State Department, said in a July 16, 2005 issue of the National Journal that the FBI is on its sixth counter-terrorism chief since 2001. "There is a rhetorical gap the size of the Grand Canyon, in which the Bush Administration on one hand insists that fighting terrorism is the No. 1 priority, and yet as far as personnel goes, it is treated as the last priority."

a. List the names of each of the FBI counter-terrorism chiefs, with their dates of service in this position and the reasons for their departure. Include as an attachment to this response all internal documents that set forth the reasons for the departure including, but not limited to, employment records. Provide a résumé, curriculum vitae or biography of each of the persons who held this position.

Response:

Following are the assignment histories of each Assistant Director (AD) of the FBI's Counterterrorism Division (CTD). Please note that before 11/21/1999, counterterrorism (CT) was part of the National Security Division, which became the Counterintelligence Division (CD) following an FBI reorganization (these assignments are referred to below as assignments to the CD).

Dale L. Watson
Entered on duty as a Special Agent (SA) on 2/12/78.
Assigned to Birmingham Division on 5/20/78.
Reassigned to New York on 10/19/82.
Reassigned to CD, FBI Headquarters (FBIHQ) on 1/6/85.
Promoted to Supervisory Special Agent (SSA), CD, on 1/19/86.
Reassigned to Washington Field Office (WFO) on 3/11/87.
Promoted to Unit Chief (UC) in the Criminal Investigative Division (CID) on 11/25/91.
Reassigned to CD UC on 4/23/92.
Promoted to Assistant Special Agent in Charge (ASAC), Kansas City Division, on 5/3/94.
Reassigned to CD as a GS-15 SSA on 9/1/96 and detailed to the National Security Agency.
Promoted to Section Chief (SC), CD, on 12/13/96.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00061 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.002

Promoted to Deputy Assistant Director (DAD), CD, on 7/8/98.
Promoted to AD, CTD, on 12/14/99.
Promoted to Executive Assistant Director (EAD), CT/Counterintelligence (CI), on 12/2/01.
Retired on 9/30/02.

Pasquale J. D'Amuro
Entered on duty as an SA on 5/6/79.
Assigned to the New York Division on 8/22/79.
Promoted to SSA on 2/15/87.
Assigned as Assistant Inspector, Inspection Division, on 4/30/95.
Promoted to GS-15 SSA, CID, on 7/8/96.
Reassigned as ASAC-CT, New York Division, on 8/31/97.
Promoted to Associate SAC, New York Division, on 1/29/01.
Promoted to AD, CTD, on 1/29/02.
Promoted to EAD, CT/CI, on 11/14/02.
Reassigned as Assistant Director in Charge (ADIC), New York Division, on 8/4/03.
Retired on 3/31/05.

Larry A. Mefford
Entered on duty as an SA on 8/6/79.
Reassigned to Sacramento Division on 11/23/79.
Reassigned to Los Angeles Division on 9/15/80.
Reassigned to WFO on 12/21/86.
Reassigned to the Critical Incident Response Group on 9/27/87.
Promoted to SSA, CID, on 11/5/89.
Reassigned to Minneapolis Division on 4/6/92.
Reassigned to San Francisco Division as an SA on 7/9/95.
Promoted to SSA, San Francisco Division, on 5/11/97.
Promoted to ASAC, San Diego Division, on 9/27/98.
Promoted to Associate SAC, San Francisco Division, on 6/12/00.
Promoted to AD, Cyber Division (CyD), on 5/28/02.
Reassigned as AD, CTD, on 11/22/02.
Promoted to EAD, CT/CI, on 8/18/03.
Retired on 10/31/03.

John S. Pistole
Entered on duty as an SA on 9/18/83.
Assigned to Minneapolis Division on 1/6/84.
Reassigned to New York Division on 4/7/86.
Promoted to SSA, CID, on 11/30/90.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00062 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.003

Reassigned to Indianapolis Division on 3/21/94.
Promoted to ASAC, Boston Division, on 7/4/99.
Promoted to Inspector on 7/23/01.
Promoted to DAD, CTD, on 6/3/02.
Promoted to AD, CTD, on 9/16/03.
Promoted to EAD, CT/CI, on 12/22/03.
Promoted to Deputy Director on 10/3/04 (current position).

Gary M. Bald
Entered on duty on 9/11/77 and assigned to the Criminal Justice Information Services (CJIS) Division as a fingerprint examiner.
Reassigned to the Laboratory Division as a physical science aid on 4/24/78.
Promoted to cryptanalyst on 10/23/78.
Became an SA on 4/19/81.
Assigned to Albany Division on 8/10/81.
Reassigned to Philadelphia Division on 3/31/84.
Promoted to SSA, Inspection Division, on 6/4/89.
Reassigned to Newark Division on 8/9/91.
Promoted to GS-15 Assistant Inspector, Inspection Division, on 4/16/95.
Reassigned as UC, CID, on 9/3/96.
Promoted to ASAC, Atlanta Division, on 12/2/96.
Reassigned as Inspector-in-Charge on 2/25/00.
Promoted to SAC, Baltimore Division, on 9/30/02.
Promoted to DAD, CTD, on 11/17/03.
Promoted to AD, CTD, on 3/4/04.
Promoted to EAD, CT/CI, on 11/2/04 (current position).

Willie T. Hulon
Entered on duty as an SA on 9/6/83.
Assigned to Mobile Division on 12/22/83.
Reassigned to Chicago Division on 1/28/86.
Reassigned to San Antonio Division on 4/11/88.
Promoted to SSA, San Antonio Division, on 10/20/91.
Reassigned to CID on 3/19/95.
Promoted to GS-15 Assistant Inspector, Inspection Division, on 2/4/96.
Reassigned as UC, CID, on 6/2/97.
Promoted to ASAC, St. Louis Division, on 3/9/98.
Promoted to Inspector on 11/3/00.
Promoted to Chief Inspector on 7/26/01.
Promoted to SAC, Detroit Division, on 12/3/02.
Promoted to DAD, CTD, on 6/7/04.
Promoted to AD, CTD, on 12/26/04 (current position).

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00063 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.004

b. Provide a statistical report of the number and percentage of FBI human resources assigned solely and entirely to the Counter-Terrorism Division of the FBI.

Response:

The response to this inquiry is classified and is, therefore, provided separately.

2. How much of the FBI's resources are dedicated to intelligence, as opposed to prosecutorial, work?

a. What percent of your human resources are assigned full-time to intelligence gathering as opposed to the prosecutorial support role?

Response:

Intelligence is integrated into all aspects of the FBI's law enforcement mission, and is both an investigative tool and a mission unto itself. Intelligence is also a key objective that is pursued during the prosecutorial phase of an investigation. For this reason, it is difficult to answer this question without a clear context. The resources devoted to intelligence as a mission in and of itself (as opposed to intelligence used and produced in the context of an investigative mission) fall, as an accounting matter, within the FBI's Intelligence Decision Unit (IDU). Of the positions included in the FBI's Fiscal Year (FY) 2005 Congressional appropriation (including the FY 2005 supplemental), 15.5 percent are included in the IDU. These positions include the staff assigned to the Directorate of Intelligence (DI) and personnel under the programmatic control of the EAD for Intelligence (EAD-I), as well as a pro rata share of operational, investigative, management, and other support personnel (such as finance, human resources, and legal personnel) who support the intelligence mission.

We stress, however, that no neat dividing lines distinguish intelligence from law enforcement activities. Intelligence is a core investigative tool, and a valuable product of the prosecutorial phase of an investigation.

b. What is the number of full-time equivalents (FTEs) in Intelligence?

Response:

The FBI's FY 2005 Congressional appropriation included 4,365 full-time equivalents in the IDU.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00064 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.005

c. What percent of your monetary resources are used in intelligence?

Response:

16.5 percent of the FBI's FY 2005 Congressional appropriation (including the FY 2005 supplemental) is included in the IDU.

3. Director Mueller stated in a recent speech: "The development of the National Security Service ("NSS") is the next step in the evolution of our ability to protect the American public."

a. What plans, policies and strategies has FBI implemented toward this goal?

Response:

The FBI will submit its National Security Branch Implementation Plan to the President shortly. This Plan is being coordinated with the Office of the Director of National Intelligence (ODNI), and several issues must be resolved before submission. In response to the President's six specific instructions, the Plan provides statements of principle from which detailed implementation plans will be developed. As articulated in the Plan, the National Security Branch (NSB) will strengthen the FBI's existing capabilities in these areas by combining the CTD, CD, and DI into an integrated service that effectively leverages the assets and abilities of all three entities. The NSB will be headed by an EAD.

b. Set forth the process by which FBI and Director Negroponte will appoint the head of the NSS.

Response:

The President has directed that the head of the NSB be appointed with the concurrence of the Director of National Intelligence (DNI), and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directs that the Attorney General obtain the concurrence of the DNI before appointing an individual to the position of EAD for Intelligence or any successor position created through reorganization. Because the head of the NSB (the EAD-NSB) is the successor to the EAD-Intelligence position, the FBI Director forwarded to the Attorney General his recommendation for appointment to the position of EAD-NSB. Consistent with the IRTPA, the Attorney General sought the concurrence of the DNI before making the appointment.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00065 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.006

The FBI Director recommended Gary M. Bald, EAD for CT/CI, for appointment as the EAD-NSB. This recommendation was approved by the Attorney General, and the DNI concurred in the appointment. The Deputy appointed to assist EAD Bald in directing the NSB is Philip Mudd from the Directorate of Operations at the Central Intelligence Agency (CIA).

4. Joint Terrorism Task Forces (JTTFs) were set up to coordinate counterterrorism activities between the FBI, state and local law enforcement agencies. The 9/11 Commission Staff Report no. 9 (pg. 10) states that most local and state law enforcement representatives to the JTTFs were simply liaisons and did not fill management or investigative positions.

a. Are there currently any non-FBI officials in management positions in any JTTFs?

Response:

At the discretion of the ADIC or SAC (while most Field Divisions are led by SACs, very large FBI Field Divisions are led by ADICs), participating agencies that have devoted significant numbers of employees or resources to a Joint Terrorism Task Force (JTTF) may assign supervisory personnel to handle administrative matters for their employees. Presently, the New York JTTF includes the largest number of management level non-FBI officials (a New York Police Department (NYPD) deputy chief, captains, lieutenants, and sergeants). These are not operational management positions, but are instead filled by personnel managers for the 115 NYPD employees assigned to the New York JTTF. Management-level officials are also assigned to many other JTTFs for the same purpose. In addition, each JTTF has an Executive Board that is chaired by the FBI's ADIC or SAC and is composed of senior federal, state, and local law enforcement officials who review the operations of the JTTF and provide input and recommendations as to the JTTF's investigative direction.

b. If not, why not?

Response:

For command and control purposes, the FBI ADIC or SAC is a JTTF's overall commander and is responsible for the operational and administrative matters directly associated with that Division's JTTF(s). The operational chain of command (in "top down" order) is as follows: ADIC (if applicable), SAC, ASAC, and SSA. Staffing issues are the responsibility of the FBI chain of command, while the SSA, as the JTTF Supervisor, supervises JTTF operational

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.007

activities. All JTTF investigations are opened and conducted in conformance with FBI policy.

c. If so, set forth the name, location and position of such non-FBI official.

Response:

Although many JTTFs include non-FBI members in management-level positions with respect to members of their organizations, none are in operational management positions. In the largest New York JTTF, as with other large JTTFs, the staff of each operational squad includes an NYPD sergeant who collaborates with the FBI squad supervisor regarding investigative decisions. This collaboration also occurs among more senior managers, where NYPD lieutenants, captains, and higher share decision making with FBI executive managers. This enhances investigative oversight, which contributes to a more effective CT effort. Ultimately, though, the FBI is responsible for ensuring investigations are conducted in accordance with all aspects of federal law, Attorney General Guidelines, and Department of Justice (DOJ) and FBI policy.

d. How many JTTFs exist today and how many FBI personnel are assigned full time to each JTTF?

Response:

Currently, the 103 JTTFs are staffed by a total of 3,714 full-time law enforcement officers, including 2,196 FBI SAs, 683 officers from other federal agencies, and 835 state and local law enforcement officers.

5. A July 19, 2005 *New Yorker* article entitled "*Defending the City*" describes the FBI agents assigned to an NYPD counterterrorism center as "young white men ... standing stiffly against a wall."

a. What kind of interaction do you expect from your agents detailed to local counterterrorism centers?

Response:

FBI personnel assigned to local or regional CT centers or to Regional Intelligence Centers (RICs) are expected to be fully engaged, along with other federal, state, and local agencies, in accomplishing the center's mission. FBI personnel are assigned to these centers to facilitate an unimpeded flow of information concerning terrorism threats and intelligence between the centers and the JTTFs,

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.008

which are the primary operational and investigative arms of the U.S. Government in the war on terrorism. Coordination between regional CT centers, RICs, the FBI's CTD, and other appropriate entities is accomplished through those assigned or detailed to the JTTFs and to Field Intelligence Groups (FIGs).

b. Does the FBI plan to make the efforts of municipal law enforcement agencies an integrated part of their counterterrorism operations, contrary to what is being reported?

Response:

The FBI currently incorporates the efforts of municipal, state, and other federal agencies in CT operations because it has found that success against terrorism is best achieved through cooperation among federal, state, and local law enforcement and public safety agencies. The FBI formed the JTTFs to maximize interagency cooperation and coordination and to create cohesive units capable of drawing on resources at all government levels in responding to terrorism threats. Currently, the 103 JTTFs are staffed by 3,714 full-time law enforcement officers (including 835 state and local law enforcement officers) and augmented by 1,355 part-time law enforcement officers, including 121 FBI SAs, 708 officers from other federal agencies, and 526 state and local law enforcement officers.

c. If so, what specific plans does the FBI have to more fully integrate their agents into these centers?

Response:

FBI ADICs and SACs are encouraged to interact with and participate in regional CT centers and RICs in their territories. While there may not be a regional CT center or RIC in every ADIC's or SAC's territory, all FBI field offices currently manage and operate FIGs, which serve as the central intelligence component of every FBI Field Office and perform the office's core intelligence functions. The primary mission of these FIGs, which are predominantly staffed by FBI intelligence analysts (IAs), is to provide direct operational and strategic analytical support to the JTTFs. The FIGs and JTTFs both have roles in ensuring that intelligence collected by the JTTF is properly and timely disseminated to intelligence customers.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.009

d. Has anyone within FBI Headquarters investigated these assertions made in the *New Yorker* article and has any corrective action been taken?

Response:

While the FBI is aware of this article, no changes or adjustments to the FBI's operating procedures have been made as a direct result of the claims made in the article.

6. The FBI often seems reluctant to share pertinent information with local and state law enforcement agencies. The *New Yorker* article cites an instance in October 2001 when the White House was informed that a 10-kiloton nuclear weapon was being smuggled into New York City (p. 61). Mayor Giuliani and the NYPD were not informed of this threat. Today, the NYPD complains that while the flow of information has improved, integrated intelligence sharing does not yet occur. What is the FBI doing to actively improve the flow of terrorism information between the FBI and state and local law enforcement agencies?

Response:

The FBI takes such criticisms very seriously and is implementing a three-pronged strategy to improve the flow of information through policy, organization, and technology. The FBI shares classified intelligence and other sensitive FBI data with federal, state, and local law enforcement officials through a variety of means, including the JTTFs, which partner FBI personnel with investigators from federal, state, and local agencies and are important force multipliers in the fight against terrorism. Since 9/11/01, the FBI has increased the number of JTTFs from 35 to 103 nationwide and has established the National Joint Terrorism Task Force (NJTTF) at FBIHQ, staffed by representatives from 38 federal, state, and local agencies. The NJTTF's mission is to enhance communication, coordination, and cooperation by acting as the hub of support for the JTTFs throughout the United States, providing a point of fusion for intelligence acquired in support of CT operations. The FBI agrees that effective information flow is critical and will continue to create new avenues of communication among law enforcement and intelligence agencies to better fight the terrorist threat.

The FBI's policy is to share by rule and withhold by exception. For example, while the FBI is committed to ensuring that its most sensitive law enforcement and intelligence sources and methods are protected from unauthorized disclosure, this is accomplished by sanitizing documents containing this information and then disseminating the resulting unclassified documents, rather than by merely withholding the unsanitized documents. The FBI has created a senior-level policy group, the Information Sharing Policy Group (ISPG), to ensure the framework

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.010

exists to facilitate compliance with the emphasis on broad dissemination. The ISPG is co-chaired by the FBI's EAD-I and EAD-Administration, and brings together the FBI entities that generate and disseminate law enforcement information and intelligence. Since its establishment in February 2004, this body has provided authoritative FBI policy guidance for internal and external information sharing initiatives. Working in conjunction with the Chief Information Officer (CIO) and his Program Management Executive (PME), the ISPG integrates information technology initiatives with FBI mission objectives, policy guidance, and legal authorities.

The FBI has also made technological and organizational changes to improve the flow of terrorism information between the FBI and state and local law enforcement agencies. Through our National Information Sharing Strategy (NISS), the FBI is implementing new technological tools to facilitate the sharing of regional and national criminal data with law enforcement agencies. NISS has three components: National Data Exchange (N-DEx), Regional Data Exchange (R-DEx), and Law Enforcement Online (LEO). N-DEx is the first national information sharing service. It will collect and process crime data from all major FBI databases, including the National Crime Information Center (NCIC), and will combine and correlate data to permit "one-stop shopping." N-DEx will give users access to information that will assist them in detecting and preventing terrorist attacks, in linking cases, and in forming broader investigative partnerships. Currently, N-DEx is in the pilot phase of operations, with full capability anticipated in 2007.

As a complement to N-DEx, R-DEx will enable the FBI to share data, including documents from its investigative files, electronically across federal, state, and local boundaries, improving the ability to prevent terrorism and other crimes by supplying the tools for using information in new analytical ways. R-DEx will also dramatically reduce the time spent by analysts in routine data entry, collation, and manual data manipulation by providing integrated information for use by all law enforcement agencies and by facilitating the analysis of law enforcement information, including queries, associations, and linkages to automated reports. The first R-DEx regional systems are in St. Louis and Seattle.

LEO, the third NISS component, uses Web-based communications capabilities to permit the law enforcement community to exchange information, conduct online education programs, and participate in professional special interest and topically focused dialog. LEO, which has been operational since 1995 and presently serves more than 42,000 users, has secure connectivity to the Regional Information Sharing Systems network. FBI intelligence products are disseminated weekly through LEO to more than 17,000 law enforcement agencies, providing

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00070 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.011

information about terrorism, criminal, and cyber threats to patrol officers and other local law enforcement personnel who have direct daily contacts with the general public. Enhancements have permitted LEO to serve as the primary channel for Sensitive But Unclassified communications with other federal, state, and local agencies. The FBI also uses LEO to share intelligence products with Homeland Security Information Network (HSIN) users; states and major urban areas use the secure HSIN to obtain real-time interactive connectivity with the Homeland Security Operations Center and to share information with other HSIN users at the Sensitive But Unclassified level.

In addition to these technological enhancements, the FBI has also made organizational changes to enhance coordination with state and local law enforcement authorities. Among these was the establishment, in April 2002, of the Office of Law Enforcement Coordination (OLEC). Headed by a former state police chief, OLEC is responsible for ensuring that relevant intelligence is shared, as appropriate, with state and local law enforcement. As outlined in the FBI's Intelligence Policy Manual, the DI also shares information with our partners in state and local law enforcement through Intelligence Information Reports, Intelligence Bulletins, and Intelligence Assessments.

In September 2003, the FBI also established FIGs in all Field Divisions. FIGs centrally manage the intelligence production and dissemination in FBI field offices, ensuring that state, local, and tribal law enforcement partners receive all relevant intelligence to support their missions. Among the key initiatives in this area is the joint development of intelligence requirements, along with state, local, and tribal partners, that clearly convey to FIGs the needs of those partners. In addition, in August 2005 the FBI worked with the Global Intelligence Working Group Requirements Subcommittee to develop a standing set of intelligence requirements for the United States Intelligence Community (USIC) and state, local, and tribal law enforcement with respect to national security and criminal intelligence topics. Once approved by the Criminal Intelligence Coordinating Council, this document will serve as the principal guidance for intelligence sharing between the FBI and other law enforcement organizations.

For information concerning the role of the Terrorist Screening Center (TSC) in sharing this important information, please see the response to Question 46.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.012

7. In recent articles in the *New York Times* and other news sources, municipal police chiefs from New York, Los Angeles, Washington, D.C., Chicago, and Las Vegas repeatedly cite the FBI's unwillingness to share raw intelligence on a regular basis with their departments that would allow them to focus on the immediate threats in their cities. Washington Metropolitan Police Chief Ramsey stated, "I don't need a threat assessment. I need to know what I can do to proactively strengthen the security of our transit system." Is the FBI willing to allow local police departments' regular and immediate access to raw intelligence that is related to counterterrorism efforts in their jurisdictions?

Response:

As indicated in response to Question 6, above, the FBI has taken affirmative steps to improve the quantity and quality of shared raw intelligence, and we will continue to seek ways of improving that process.

8. Municipal police chiefs across the U.S. are discussing the formation of a nation-wide municipal counterterrorism network to supplement the flow of information from the FBI and DHS. Much of the discussion of this network has centered on the NYPD model of stationing agents in overseas countries to gather instant information that the FBI and DHS deliver hours or days later.

a. Does the FBI support this effort by local law enforcement to create its own national counterterrorism network?

Response:

The FBI considers state, local, and tribal law enforcement to be core nodes in the national CT network. We believe it is essential that such a network be part of the larger U.S. Information Sharing Environment (ISE), which is established under the direction of the ISE program manager pursuant to section 1016 of the IRTPA. Information sharing is crucial in the war on terrorism, and the FBI works with and participates in many of the regional fusion centers and other information sharing ventures that have already been established to ensure both that information from the national level is shared with state, local, and tribal law enforcement and that information developed by local law enforcement agencies is disseminated and shared with the national CT community, as well as with our foreign allies under appropriate circumstances.

The FBI defers to the Department of State for a judgment concerning the extent to which independent activities of state, local, and tribal law enforcement networks overseas may complicate U.S. foreign policy.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.013

b. Does the FBI view this movement towards a national municipal counterterrorism network as a failure in their intelligence dissemination network?

Response:

The FBI does not view this initiative as a failure, but instead as a vital part of the nation's ISE.

c. What plans does the FBI have to fix this perceived problem?

Response:

The FBI's strategy to improve the flow of information through policy, organization, and technology is articulated in response to Question 6, above.

9. The FBI's lack of promptly sharing important terrorist information is so well known, that CNN uses the fact that local police obtain information sooner from CNN than from the FBI or DHS as a marketing tool in a prime-time commercial quoting local law enforcement that they receive their first information on terrorist activity from CNN.

a. Provide any written internal memoranda referring to this commercial and any written or oral response made by any FBI personnel to CNN.

Response:

We are aware of neither written internal memoranda referring to the commercial nor written response to CNN. We are also not aware of any oral discussions between the FBI and CNN regarding the commercial.

b. Provide a copy of any written communication and a written summary of any oral communication with any local law enforcement agents concerning this commercial.

Response:

Both oral and written communications with local law enforcement officials are frequent and wide ranging. While no such communications regarding the CNN commercial have come to the attention of senior FBI officials, we have no way of knowing whether informal communication on this topic has occurred.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.014

10. The creation of the Information Sharing Environment ("ISE") has been described by some as marginalizing the responsibilities of the Department of Homeland Security by giving the information-sharing responsibilities of the federal government to a new agency.

a. How does FBI expect to interact with the ISE and what, if any, does FBI see as the role of the Department of Homeland Security in terrorist information sharing?

Response:

The FBI does not view the creation of the ISE as marginalizing the responsibility of any federal agency, including the Department of Homeland Security (DHS), and believes DHS's information-sharing role is defined in the Homeland Security Act of 2002. The ISE, specifically the ISE program manager, will establish information sharing technical standards and policies. The day-to-day sharing of content will occur in consonance with these standards, but will be accomplished by the individual agencies that comprise the U.S. CT network. The FBI expects to play a significant role in the ISE, including through the information sharing strategies discussed in response to Question 6, above, and will adjust its technical standards and policies to conform with those of the ISE.

Through the DI, the FBI has established FIGs in all field offices to ensure that terrorism intelligence needed by other agencies is extracted from investigative reports and disseminated to those agencies. This dissemination occurs at all levels of classification through direct message traffic and Web-based networks classified at the Top Secret-SCI level, the Secret level, the Sensitive But Unclassified level, and the Unclassified level. All FBI systems, networks, and communications channels will become part of the national ISE under the framework being developed by the ISE program manager, and the FBI is committed to using this framework to share as much terrorism information as possible. This commitment is reflected in the issuance of an Intelligence Policy Manual that provides specific guidance and emphasizes techniques to assist analysts in writing for dissemination.

The FBI does, however, remain committed to enforcing access controls to protect its most sensitive law enforcement and intelligence sources and methods from unauthorized disclosure in appropriate circumstances (such as when unauthorized disclosure would present a grave risk of compromise to the FBI's ability to obtain information about difficult collection targets). To maintain such protection, information may be disseminated in sanitized or declassified versions that are more easily used and shared by recipients.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.015

b. How many employees does FBI plan on providing to ISE as "detailees?" If any, when and who will FBI provide?

Response:

The FBI is working with DOJ, the DNI, and the ISE program manager to determine the appropriate number of detailees, as well as their skill mix.

c. What other resources does FBI expect to provide to ISE and when?

Response:

Both DOJ and the FBI are prepared to offer any and all of our information technology and content to the ISE program manager, and are working with the program manager to ensure the appropriate integration of those resources into the ISE.

11. The FBI has in the past three years spent over $170 million dollars on the Virtual Case File system (VCF), only to recently inform the American people that all of their tax dollars were spent with nothing to show. Now the FBI has announced the all new Sentinel program as the system to fix all of their programs.

a. What specifically will happen that will ensure that Sentinel will not be another multi-million dollar fiasco?

Response:

As the FBI advised during the hearing, we recognize that the development of Virtual Case File (VCF) suffered from inadequate managerial control and changing technical requirements. Using a disciplined programmatic approach in Sentinel's development will allow us to leverage the lessons learned from that effort.

Among other things, this programmatic approach has led to the development of a new Life Cycle Management Directive (LCMD), which specifies numerous criteria for passage through strict control gates. Each step of the process is approved by an appropriate Information Technology (IT) governing board, as outlined in the LCMD, before the program can progress to the next step. This process is discussed further in response to Question 11e, below. Several other key factors will also contribute to the success of the Sentinel program.

- The assignment of dedicated, experienced program oversight personnel.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.016

• Early formation of processing teams comprised of both government and contractor representatives.

• Rigorous application of Earned Value Management System (EVMS) controls (discussed in response to Question 11e, below).

• Award of the contract to a "best value" contractor – one with dedicated, experienced personnel and a proven track record.

• A disciplined award-fee contract process.

• A rigorous "change control" process to reduce technical requirement revisions.

In addition, the following efforts should significantly improve the efficiency and effectiveness of the Sentinel development process.

• Commercial off-the-shelf software will be used whenever possible to decrease development and maintenance expenses, time, and risk.

• The use of a modular, loosely coupled architecture will allow the easy replacement of components. A failure of one component will not cause the whole system to fail, which will reduce overall program risk. If necessary, individual commercial products can be quickly and easily replaced with other comparable products with minimal impact on the whole system. This modular design will also facilitate component upgrades and replacements as newer versions evolve.

• The flexible architecture will allow for rapid re-configuration if the FBI's business needs change.

• The use of prototypes of key Sentinel components (workflow, portals, and security managers) will permit the identification of potential integration issues before they would be encountered through a fully deployed Sentinel program. The use of these prototypes will also allow early user feedback, reducing the risk that Sentinel will not meet users' needs. Permitting operational users access to the prototypes before Sentinel is fully developed and deployed will also provide early operational benefits.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.017

b. Provide copies of FBI Request for Proposals and any responses thereto regarding the Sentinel program.

Response:

The Sentinel Statement of Work is attached (Enclosure A).

Responses to the RFP constitute "source selection information" as defined by 41 U.S.C. § 423(f)(2), release of which is generally prohibited by law (41 U.S.C. § 423(a)). Because the disclosure of this information would jeopardize the integrity of the procurement process, and because information from vendors is proprietary to them and not the Government's information, we decline to disclose those responses.

c. What is the FBI budget for this new system?

Response:

The FBI has developed a cost estimate to be used for budgetary purposes, but revealing it would alert potential contractors to the government's expectations regarding contract price, which would compromise the ability of the source selection process to identify the lowest responsive, responsible bidder. The FBI will have a final cost estimate when the contractor is selected.

d. Provide the schedule of expected milestones in this project.

Response:

The time frames in which milestones will be completed is a matter that will be addressed through the contract bid process, so the schedule will not be determined until the contract is awarded (in fact, the schedule will not be finalized until the completion of a review scheduled to occur 6 weeks into the first phase). While the schedule will continue to be notional at the time of contract award, we would be pleased to provide it to the Committee at that time.

The attached chart (Enclosure B) depicts four notional phases, including project reviews, control gates, and other controls associated with each phase.

Phase I establishes a single point of entry for legacy case management; expands the search capability to include IntelPlus file rooms; provides browser access to investigative data without requiring that browsers understand the changes in system architecture; and subsumes and expands current Web-based Automated

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.018

Case Support (ACS) capabilities by summarizing a user's workload on a dashboard, rather than requiring the user to perform a series of queries to obtain it. To simplify data entry into the Universal Index (UNI), an entity extraction tool will be used to automatically index appropriate persons, places, and things. Finally, the core infrastructure components will be selected during this phase, and may include an Enterprise Service Bus and foundation services.

Phase II provides case document management and a records management repository, beginning the transition to paperless case records and implementing electronic records management. A workflow tool will support the flow of electronic case documents through their review and approval cycles, and a new security framework will support role-based access controls, single sign on, externally controlled interfaces, and electronic signatures based on Public Key Infrastructure. This phase addresses the concerns of the users of Sentinel's Initial Operating Capability that a paperless environment is necessary to leverage the benefits of automated workflow.

Phase III replaces and improves the Bureau-wide global index for persons, places, and things. In the "Connect the Dots" paradigm, the "dots" are represented by UNI, the legacy index that is, in effect, a database of entities (i.e., persons, places, and things) that have case relevance. Unlike the current UNI index, which supports a limited number of attributes, the new global index will improve the richness of the attributes associated with the indexed entities, permitting more precise searching.

Phase IV implements the new case and task management and reporting capabilities and will begin the systematic consolidation of case management systems.

e. Provide the system by which each stage of production of the program will be measured.

Response:

As indicated in response to Question 11d, above, the Sentinel program is employing a multi-tiered system of program management tools and practices to measure each stage of system development. Following are the three major program management tools and practices to be used by the Sentinel program.

1. Adherence to and expansion of the oversight process outlined in the FBI's IT LCMD. During each of the four phases of the Sentinel system's development, independent, senior executive boards will conduct six

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.019

separate control gate reviews. Each of these reviews must be favorable before Sentinel development can proceed. Each phase of the Sentinel system's development will also be the subject of 12 program-level reviews to measure that phase's progress. The standard FBI IT LCMD oversight and management process has been expanded for Sentinel by additionally requiring:

• An Acquisition Plan Review by the FBI Investment Management/Project Review Board before awarding contract options for Phases II, III, and IV.

• An Integrated Baseline Review immediately following the award of the base contract and each contract option to ensure EVMS policies and procedures are in place and adequate.

• A Delivery Acceptance Review near the end of each phase of Sentinel development to ensure that all work has been completed properly, including the training of field personnel and the accomplishment of organizational change management tasks.

2. Adherence to the use of EVMS principles and practices recommended by the Program Management Institute and Defense Acquisition University and mandated by the Office of Management and Budget. The Sentinel Program has embraced and mandated the use of EVMS principles and practices to measure the progress of each phase against an EVMS baseline (cost, schedule, and performance). The Sentinel Statement of Work requires that the provisions of FAR Case 2004-019 (published in the *Federal Register* on 4/8/05) be followed. Among other things, this requires the prime contractor to furnish a monthly progress report with respect to each phase's EVMS baseline and must provide the reasons for variances of more than five percent.

3. Use of an Independent Validation and Verification (IV&V) authority. Each phase of the Sentinel system's development will be independently measured and reported on by an IV&V authority. Throughout the development and deployment contract, this independent authority will measure progress and performance against the performance baseline. The results of these independent measurements will be reported to the FBI's CIO and PME.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.020

12. The 9/11 Commission Staff Report no. 9 (pg. 9) faulted the FBI for having poorly trained and unqualified analysts.

a. Has the FBI changed its policy of hiring internally? Has there been any policy change that would allow for and that has resulted in the hiring of educated, trained and experienced analysts from external sources?

Response:

The 9/11 Commission's criticism of the qualifications of FBI analysts was based on an internal FBI document published in 1998 that asserted that two-thirds of FBI analysts were not qualified. The basis for the judgment expressed in that document is unclear and, in any event, is no longer accurate. In the 7 years since its publication, the FBI has established policies and systems to ensure the FBI's IAs are of the highest competence and quality. With the benefit of these new policies and systems, over the past two years we have hired more than 1,100 IA applicants possessing one or more critical skills. Of these recent hires, 59% had related intelligence or analytical experience, 47% had military experience, and 38% had advanced degrees.

A key component of this recent policy has been creation of the Intelligence Career Service (ICS), which demonstrates the importance of the FBI's intelligence mission and elevates the stature of its intelligence professionals. To develop the ICS, the FBI looked to both other elements of the USIC and the FBI's selection systems for best practices, creating a selection system implementation plan that would ensure selections based upon competencies identified for IAs, Language Analysts (LAs), and Physical Surveillance Specialists. (A "competency" is a cluster of related knowledge, skills, and abilities needed to perform a specific job.) These competencies correlate with job performance, can be measured against standards, and can be improved through training and development. Competency models allow for maximum reuse of human resources tools (such as testing and training courses) to assess and develop commonly required skills. Competency models also allow for the development of unique tools to assess and develop specialized skills. The competencies define our selection and hiring, training and development, performance management, Intelligence Officer Certification, retention, and career progression. They also help target and assess applicants, including those from within the FBI, with critical skills in intelligence, foreign languages, technology, area studies, and other specialties.

In furtherance of the effort to attract and retain IAs with critical skills, the FBI has also implemented three scholarship programs:

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.021

1. The Pat Roberts Intelligence Scholarship Program (PRISP) enhances the FBI's retention of IAs with specialized critical skills. Through the PRISP, the FBI can grant $25,000 scholarships to current employees to help fund their past, current, or future studies in specialized skills or areas deemed critical by the FBI.

2. The Cooperative Education Program offers to college juniors and seniors who are pursuing studies in critical Intelligence Program skills the opportunity to attend school full-time during part of the year and work at the FBI full-time during part of the year. Program participants receive FBI salaries and benefits, as well as tuition assistance.

3. The Educational Attainment Internship provides financial assistance to selected high school seniors who will be pursuing college level work in a discipline deemed operationally critical to the FBI.

b. How many analysts have been hired since 9/11 from external sources?

c. How many analysts have been hired since 9/11 from internal sources?

Response to subparts b and c:

As indicated below, FBI records indicate that from FY 2002 through 8/18/05 the FBI has hired 377 IAs from within the FBI and 958 from outside the FBI (the number of external hires may include some FBI personnel who applied to external job postings). Regardless of the source of the candidate, all IA candidates are selected according to the same competency-based criteria, and successful IA candidates must meet these criteria.

Fiscal Year	Internal Sources	External Sources
2002	56	40
2003	77	173
2004	141	208
2005 (thru 8/18/05)	103	537

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.022

13. Since 9/11, the FBI continued to be plagued by a shortage of qualified analysts and translators. In the *New Yorker* article, the New York Police Department (NYPD) was able to resolve their analyst and translator problem by drawing upon immigrants who were intimately familiar with the languages and cultures under survey (pg. 64). These languages included Farsi, Arabic, Pashto, Dari and 60 other languages.

a. Has the FBI launched a similar program to address this issue?

b. If not, why not?

Response to subparts a and b:

For the last several years, the FBI has aggressively recruited from ethnically diverse communities throughout the United States to meet its translation requirements. In addition to traditional media campaigns, the FBI's National Recruiting Team and DI personnel have targeted specialty conferences, career fairs, university foreign language departments, and other forums to recruit those with critical language skills. FBI management officials also regularly host community meetings and speak at local events to generate interest in FBI employment and contractor opportunities. Beyond this, the FBI has partnered with organizations such as the U.S. Copts Association, Arab American Anti-Discrimination Committee, Arab American Institute, Network of Arab American Professionals, and Muslim Public Affairs Council to establish good will with their membership and to encourage those with critical language skills to consider FBI employment. Collectively, these efforts have resulted in more than 80,000 applications for linguist positions since 9/11/01 (most often, FBI linguists begin as contract linguists, so the majority of these applications have been for contract linguist positions that often evolve into FBI employment as LAs).

More than 3,000 FBI employees and contractors, including 397 LAs and 1,004 contract linguists, now have certified foreign language proficiency scores at or above the working proficiency level. More than 95% of the FBI's linguists are native speakers of a foreign language. These native-level fluencies and long-term immersions in foreign cultures ensure firm grasps of not only colloquial and idiomatic speech but also of heavily nuanced language containing religious, cultural, and historical references. Trustworthiness, as demonstrated through the security clearance process, is, of course, required of all FBI employees, including linguists.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00082 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.023

14. This same article reports that the CIA and Pentagon have both asked the NYPD to assist them with translations, investigations and analysis of information relating to national security (pg. 64).

a. Has the FBI made use of the NYPD translation and analysis program?

b. If not, why not?

c. If so, set forth those instances in which the NYPD program has been used by FBI?

Response to subparts a, b, and c:

The FBI has not made use of the NYPD's translation and analysis program. In 2003, the FBI's Chief of Language Services met with the Deputy Commissioner of the NYPD to discuss common translation challenges and to explore the feasibility of sharing translation resources. During this meeting, the NYPD indicated that it did not want its officers and translation staff to undergo FBI polygraph examinations as a condition of their access to FBI information (the FBI requires that all candidates for its translator position submit to polygraph testing as a condition of being granted access to national security information). We understand that the CIA and Pentagon have found a means of ensuring trustworthiness without the use of polygraph examinations. We will work with both organizations to learn more about this process and will evaluate our ability to do the same.

15. The NYPD recruits immigrants from the Asia, Africa and the Pacific Islands to find qualified analysts and translators.

a. Does the FBI have a similar recruiting policy in place that targets immigrants?

b. If not, why not?

c. If so, provide statistics showing the results of this recruitment effort.

Response to subparts a, b, and c:

The FBI makes extensive use of LAs recruited from immigrant communities. We hire from those communities consistent with Executive Order (EO) 12968, "Access to Classified Information," which provides that "access to classified information shall be granted only to employees who are United States citizens"

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00083 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.024

(Section 3.1(b)). This EO substantially limits the FBI's ability to use the services of non-citizens, because nearly all of the FBI's CT and CI information in need of translation is classified at the "Secret" or "Top Secret" level. The EO does not, however, apply to state and local law enforcement agencies, who are free to establish their own standards for access to law enforcement information and may therefore obtain the assistance of immigrants without U.S. citizenship to meet translation requirements.

16. On multiple occasions the FBI has been criticized for having thousands of hours of untranslated terror intercepts, including most recently in the OIG report dated July 27, 2005. One of the FBI's reasons for the backlog of untranslated intercepts is the lack of cleared analysts and translators.

a. Would the FBI agree to certify local or state law enforcement security checks for the purpose of clearing analysts and translators to assist the FBI?

b. If not, why not?

Response to subparts a and b:

The FBI can authorize state or local law enforcement to conduct security checks of analysts and translators if those authorities conduct the checks in accordance with EO 12968. Generally, the requirements of EO 12968 are not met by state and local law enforcement agencies.

c. Is it true as the OIG reports that it takes the FBI an average of 16 months to hire a contract linguist - an increase in time from prior years studied?

Response:

An audit conducted by the DOJ Office of Inspector General (OIG) during 2003-2004 used the averages of the four applicant processing stages to determine a total cycle time of 14 months. A subsequent OIG audit adopted an entirely different methodology, including periods of time beyond the FBI's control, to determine that the total cycle time is, instead, 16 months. The difference between the 14-month and 16-month processing times is accounted for by these periods beyond the FBI's control, such as periods in which an applicant is out of the country and therefore unavailable for polygraph.

The FBI believes that the better measure of our processing efficiency is the 14-month applicant processing time. Under this methodology, a contract linguist candidate who successfully completes each stage of the employment process can

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00084 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.025

expect to remain in the process for 425 days before receiving the required "Top Secret" security clearance.

Contract Linguist Applicant Cycle (FYs 2004-2005)				
Phase	**Annual Volume**	**Pass Rate**	**Current Cycle Times (Median)**	**FY 07 Target (Approximate)**
Professional Testing	3,000	25%	158 days	60 days
Polygraph	600	58%	65 days	30 days
Background Investigation	350	85%	95 days	60 days
Security Adjudication	300	90%	107 days	30 days
Total	**270**	**13%**	**425 days**	**180 days**

All contract linguist candidates are subject to a thorough pre-contract vetting process that is both labor and time intensive. Contract linguist candidates must pass proficiency tests in both English and a foreign language. In addition, because they must be granted "Top Secret" security clearances, each candidate's pre-contract vetting process includes the following:

- Personnel security interview conducted by appropriately trained FBI SA or security personnel.
- Polygraph examination focused on the candidate's involvement in foreign counterintelligence matters, purpose in seeking FBI employment, application accuracy and thoroughness, and prior involvement in the sale or use of illegal drugs.
- Single-scope background investigation covering the most recent 10-year period of the candidate's life or longer.
- Risk analysis of the background investigation package conducted by FBI CI and/or CT subject matter experts.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00085 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.026

d. If true, how can FBI hire qualified, highly marketable, people when they must wait over a year to find out if they are going to be hired?

Response:

The FBI shares your concern. We are working to reduce the time required for the applicant vetting process from 425 days to approximately 180 days by FY 2007 through the implementation of process improvements recommended by a business process reengineering firm and the National Academy of Public Administration. Among other means to this goal, the FBI plans reduce the proficiency test cycle from 158 to 60 days by the end of FY 2006 by automating its language proficiency test instruments and using third party test centers. The FBI also anticipates reducing the background investigation and security adjudication cycles from approximately 200 days to 90 days by FY 2007 by consolidatmg background investigation functions within the Security Division and reorganizing to streamline associated activities.

e. If true, do the inevitable changes in the terrorist landscape and therefore the particular languages in need of translation, require an expedited hiring process in order to keep up with the ever changing war on terrorism?

Response:

The FBI can and often does respond to operational exigencies through the expedited processing of contract linguist candidates. For example, in 2005 several contract linguist candidates with proficiency in an urgently needed African language were recruited and fully vetted through proficiency testing, polygraph, and background mvestigation in 30 days or less. This rapid response capability, while extremely manpower intensive, ensures the FBI can quickly respond to the most critical national security requirements.

The FBI recognizes that with the ever-changing face and voice of global terrorism, we must be prepared to respond to translation requirements associated with the world's most obscure languages. Geopolitical indicators and threat forecasts provide a foundation for the FBI's translation planning.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00086 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.027

f. If untrue, how long does it take FBI, on average to hire contract linguists and is this time reasonable?

Response:

Please see our response to Question 16c, above.

17. The FBI translation program has been criticized for having excessive and unreasonably high standards when it comes to pre employment language testing. There have been newspaper articles detailing that, for instance, University Professors who teach Arabic were unable to pass the test.

a. Is the FBI testing standard [ ] too high?

b. What, if any, changes are planned in this testing process to avoid these unreasonably high testing standards?

Response to subparts a and b:

The FBI evaluates language tests in accordance with Interagency Language Roundtable (ILR) Skill Level Descriptions, approved by the Office of Personnel Management as the standards for government-wide use in 1985, and uses the Defense Language Proficiency Test, prepared by the Defense Language Institute, to test foreign language listening and reading skills. The ILR employs a scale of 0 to 5, describing Level 2 as "Limited Working Proficiency" and Level 3 as "General Professional Proficiency."

The passing score for FBI verbatim translation exams is 2+ or 3, depending on the score received in the speaking proficiency test. When applicants with knowledge of a foreign language fail a translation test it is typically because good translation requires not only proficiency in two languages but also what the ILR describes as "congruity judgment," or the ability to choose the best accurate equivalent from among possible translations.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00087 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.028

18. With the recent terrorist attacks in London, intelligence analysts are saying, and the American public is concerned, that an attack on American soil is imminent.

a. How is the intelligence community – FBI, ISE, DOJ – preparing to protect us against such an attack?

Response:

In response to the London mass transit attacks, the FBI has been assisting British authorities in their investigation and has been investigating any and all connections to the U.S. to prevent a similar attack here. One phase of this effort has been the production of an unclassified daily Intelligence Bulletin that communicates current investigative updates and other information that might be useful to state and local law enforcement authorities. Among other things, these bulletins have articulated the tactics and techniques used in the London bombings and detailed the chemical composition of the explosives used in the attacks. These bulletins have been provided to all FBI field offices and to our law enforcement partners.

b. What has the FBI learned from the London attacks that can help prevent a mass transit attack in the U.S.?

Response:

The FBI continues to investigate the London bombers' relationships and contacts, including their financial and communications links, to identify any persons who might pose a danger to the U.S. We remain concerned that the London attacks could serve as a template for an attack in the U.S. in which a few "home grown" extremists might target a metropolitan subway system using relatively small quantities of homemade explosives. The FBI is more committed than ever to working collaboratively with state and local law enforcement, who are often the most effective first line of defense in identifying and disrupting attacks.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00088 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.029

19. In testimony before the Senate Committee on Foreign Relations in 2002, President Henry Kelly of the Federation of American Scientists reported that "significant quantities of radioactive material have been lost or stolen from US facilities in the past few years." He also stated that much of this material is useful for the construction of radiological dispersion devices and dirty bombs.

a. What is the FBI doing to track and recover lost or stolen radiological material in the U.S.?

Response:

The FBI maintains a close relationship with the agencies involved in licensing the possession of nuclear/radiological material (including the Department of Defense (DoD), Department of Energy (DoE), and Nuclear Regulatory Commission (NRC)). Pursuant to the FBI's Nuclear Site Security Program, we have directed our field offices to establish close liaison with appropriate security personnel at nuclear sites in order to ensure prompt notification and response to suspicious activity, including attempts to illegally obtain nuclear or radiological material. We have also reiterated to all field offices the need for aggressive investigation of lost, stolen, or missing radioactive source material and the importance of ensuring that state and local law enforcement authorities promptly notify the FBI of such incidents. Coordination of these issues has been greatly facilitated by the development and enhancement of the JTTF program because the JTTFs, which are comprised of federal, state, and local law enforcement representatives, are invaluable assets in the sharing of information and coordination among law enforcement agencies. The FBI also participates in a number of interagency working groups at the Headquarters level in order to develop U.S. Government policy options for preparing for, preventing, responding to, and recovering from a radiological attack. These working groups have undertaken numerous tasks, including the review of existing security and licensing regulations for adequacy and appropriateness and the development of a National Source Tracking System to better account for individual radiological sources in the possession of NRC licensees, which include medical, industrial, and academic entities.

b. Provide a list of all known lost or stolen radiological material in the U.S.

Response:

The NRC-managed Nuclear Materials Event Database indicates that since January 2003 NRC licensees reported approximately 1,300 events involving lost, stolen, or abandoned radiological sources. The NRC estimates that approximately 50 percent of these radiological sources are eventually recovered.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00089 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.030

While statistics such as these may appear to indicate a significant loss of material, the majority of these incidents involve minute quantities of radioactive material present in industrial equipment used in radiography and well logging. Such equipment often contains "low hazard" material with a short half-life. While the FBI is concerned with all reports of lost, missing, or stolen nuclear or radiological material, and coordinates closely with the cognizant agencies in aggressively investigating these allegations, the vast majority of these incidents appear to be inadvertent rather than the product of criminal intent, do not pose a harm to public safety, and are therefore not considered "significant" for CT purposes.

20. There are currently seven sites in the U.S. that handle Category I special nuclear material, or nuclear material that is considered weapons-grade material.

a. What role does the FBI have in securing this material from theft?

Response:

The FBI is responsible for investigating allegations of unlawful use or possession of nuclear or radiological materials, and threats to use such materials, for terrorist or other criminal purposes. This responsibility includes all man-made radiological materials (those used in reactor operations as opposed to those that occur naturally), which may run the gamut from weapons-grade materials (Category I Special Nuclear Material (SNM)) to radiological source materials. Such misuse may be prosecuted through a variety of statutes.

DoE's National Nuclear Security Administration (DoE/NNSA) bears primary responsibility for the safety and security of its nuclear facilities, including those that handle Category I SNM. As part of its overall Nuclear Site Security Program, the FBI coordinates closely with these sites in a proactive effort to prevent terrorist or other criminal activities directed against these sites. Such efforts include both routine liaison activities (such as intelligence sharing and threat briefings) and more specialized initiatives (such as joint training and exercises that typically focus on the coordination of emergency responses to potentially disruptive incidents).

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00090 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.031

b. Is there a policy of standardized security procedures that must be followed by such facilities?

Response:

DoE/NNSA adheres to an extremely rigorous and robust protection strategy based on the sensitive nature of the assets under its purview. This protection strategy is "graded" according to the type of material handled at a given site, with Category I SNM sites afforded the highest level of protection. Further information on this subject may best be obtained from DoE.

c. If so, provide the standard security procedures and how these procedures are monitored by FBI.

d. If not, are there any written plans to do so? Provide written plans.

Response to subparts c and d:

Security countermeasures are part of each site's protection strategy. The FBI is not responsible for monitoring DoE's protection strategy per se, but we do maintain a level of interaction with DoE through regularly recurring liaison and training, and this interaction facilitates a regular review of these procedures.

21. In recent years, there have been a number of reported incidences of theft of documents and materials from Los Alamos National Nuclear Laboratory and other locations.

a. How does the FBI plan to reduce the number of thefts from these facilities?

Response:

Pursuant to 50 U.S.C. § 402a, the FBI is to be "advised immediately of any information, regardless of origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power." The FBI has initiated proactive measures in order to better protect against the compromise of classified information, specifically addressing compromises in the national laboratories. The cornerstone of these measures is the Agents in the Lab Initiative.

Pursuant to this initiative, FBI SAs are embedded in the Internal Security Office of the Los Alamos National Laboratory (LANL). These SAs possess academic

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00091 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.032

credentials in mechanical and nuclear engineering, which lend themselves to the LANL's overall scientific and research mission. The LANL's Internal Security Office is responsible for the Lab's counterintelligence (CI) and counterterrorism (CT) activities, including: the conduct of CI briefings/debriefings for LANL personnel; response to internal CI inquiries regarding LANL employees, contractors, and visitors; and the identification of potential CI and CT risks and exposures to Foreign Intelligence Services and terrorist organizations. The FBI has also assigned an experienced Sante Fe Supervisory Senior Resident Agent (SSRA) to focus on day-to-day LANL operations, permitting emphasis on espionage prevention and detection and strong partnerships with DoE and the CIA.

When FBI SAs investigate matters at the LANL, they share the resulting reports with DoE entities, including the LANL. DoE/NNSA uses these reports to develop "lessons learned" reports, identifying potential weaknesses in the internal security apparatus and providing recommendations to resolve concerns. In addition, the FBI's Albuquerque Division SAC meets regularly with the LANL Director to discuss all matters of interest. That meeting is attended by the Santa Fe SSRA and the LANL's Senior CI Official (who heads the Internal Security Office); the Santa Fe SSRA and LANL's Senior CI Official also meet separately each month to ensure maximum information sharing.

Additional information responsive to this inquiry is classified and is, therefore, provided separately.

b. Has FBI investigated these incidences?

Response:

The FBI thoroughly investigates all reports of possible theft or compromise of classified documents or materials. Previous cases have been successfully resolved and future incidents are much less likely due to the implementation of more effective and efficient administrative and security practices.

c. How many such incidences remain unsolved? Provide date, time, location and circumstances regarding such unsolved incidences.

Response:

The response to this inquiry is classified and is, therefore, provided separately.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00092 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.033

22. The NYPD currently treats all tractor-trailer and hazmat incidences as potential crime scenes, due to intelligence received about al Qaeda operating procedures.

a. Does the FBI have clearly defined procedures in place to facilitate cooperation between the FBI and local and state law enforcement officials to determine if an incident is an accident or a terrorist attack?

Response:

The FBI's responses to all threats and incidents involving potential weapons of mass destruction (WMD) or other terrorist acts include assessments of credibility and interagency coordination. Typically, FBIHQ is notified of a suspected WMD threat or incident by the FBI field office in the location of the threat or incident. Upon such notification, or when FBIHQ otherwise becomes aware of such threats or incidents, FBIHQ's WMD Operations Unit (WMDOU) provides rapid assistance to the field, including execution of the following standard operating procedures:

1. Evaluation of the initial threat assessment (that initial threat assessment is often conducted by the FBI field office).
2. Completion of a comprehensive threat assessment.
3. Coordination of FBIHQ assets for response and the provision of technical support.

WMDOU, which is responsible for developing appropriate FBI response policy for such incidents, overseeing strategic threat assessments, and coordinating assets to assist FBI field divisions in their responses to domestic WMD threats or incidents, uses the threat assessment process to identify the resources needed for response. WMDOU calls on previously identified subject matter experts in other agencies and consults with FBI scientists and the FBI's Hazardous Materials Response Unit as appropriate to the incident. These technical experts are able to respond to chemical, biological, and radiological/nuclear incidents, as well as incidents involving explosive devices. In addition, FBI field offices have designated WMD Coordinators, who are responsible for developing strong relationships with federal, state, and local crisis and consequence management agencies. WMD Coordinators also maintain liaison with a wide range of emergency responders through the JTTFs (each of which includes representatives from state and local government) and participate in operational crisis response training and exercises with state and local counterparts. During a potential terrorist incident, the FBI would notify JTTF members so the response may be coordinated appropriately with law enforcement partners at all levels.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00093 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.034

b. If so, provide a copy of those procedures and a description of all incidences in which the procedures have been implemented.

Response:

Both FBIHQ's WMDOU and FBI field offices respond to large volumes of threats, rendering it impracticable to provide an exhaustive list describing these incidents.

Homeland Security Presidential Directive 5 required the development of a National Response Plan (NRP) to align Federal coordination structures, capabilities, and resources into a unified, all-discipline, and all-hazards approach to domestic incident management. The 426-page NRP, which is available in full on DHS's website, provides the protocols for response to domestic incidents, including nuclear and radiological incidents, biological incidents, and other acts of terrorism. While much of the NRP concerns response to incidents such as the tractor/trailer and hazardous materials incidents on which this question focuses, the most relevant portions of the NRP are the Terrorism Incident Law Enforcement and Investigation Annex, the Nuclear/Radiological Incident Annex, and the Biological Incident Annex. Those three annexes are attached (Enclosure C).

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00094 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.035

Questions Posed by Senator Leahy

23. In follow up questions to a June 6, 2002, hearing, you stated that agents at headquarters should have expertise in areas to which they are assigned. This would certainly include counterterrorism officials. You also said that field supervisors should have "extensive counterterrorism experience." Recently, we learned from depositions in a civil suit that the highest level of counterterrorism officials at the Bureau do not have specific prior experience in this area, nor do they think it is important for them to possess such expertise.

a. How can we reform the FBI if it insists that traditional law enforcement experience is *all* that is needed to prevent and prosecute acts of terrorism?

Response:

We respectfully disagree with the assertion the FBI "insists that traditional law enforcement experience is *all* that is needed" to prevent terrorism. SA candidates for positions in all programs are required to demonstrate levels of experience and performance appropriate to the position, and increasingly rigorous standards are applied to progressively higher leadership levels.

Candidates for all SA mid-level management positions (generally, those at the GS-14 and GS-15 levels) are vetted through selection boards comprised of Senior Executive Service (SES) members representing priority divisions at FBIHQ, including CTD, CD, DI, CyD, and CID. For example, ASAC candidates (ASAC is a GS-15 position) are required to demonstrate competence in the following areas through the submission of two examples with respect to each area: communication, flexibility/adaptability, initiative, interpersonal ability, leadership, liaison, organizing and planning, and problem solving/judgment. Often, these examples identify the impact of the candidate's efforts on the FBI's highest priority matters, including CT accomplishments. Mid-level SA managers seeking promotion to entry level SES positions are required to submit résumés demonstrating success in five competencies: management, leadership, liaison, problem solving, and interpersonal ability. Within these competencies, candidates must show the highest levels of achievement in the FBI's top priorities. To the extent possible, these résumés also reflect successes in program areas applicable to the position being sought.

Throughout these multi-tiered vetting processes, strong managerial skills are considered critical, and subject matter expertise is considered and preferred, but is not mandatory. Typically, SAs who attain higher-level executive positions have first held other senior management positions in the FBI, such as SAC of a field

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00095 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.036

office, and through them have acquired management experience across both national security and criminal programs.

b. Do you think that law enforcement experience is sufficient? Or do you believe that expertise in counterterrorism should be a prerequisite for counterterrorism leaders of the Bureau?

Response:

After the events of 09/11/01, the FBI's top priority became the prevention of additional terrorist attacks against this nation. As part of this mission shift, we initiated the development of career paths for SAs that will require them to specialize in one of five areas: CT, CI, intelligence, cyber, or criminal. As this policy is implemented, the FBI will develop a cadre of SAs with subject matter expertise in each of these priority programs. Once this cadre is established, it may be appropriate for the FBI to consider mandatory subject matter expertise in certain positions. In the meantime, we believe it is appropriate to consider subject matter expertise as a factor, but not a prerequisite, when determining assignments.

Among the FBI's efforts to foster growth in these priority areas is a rotational program pursuant to which SAs are assigned to FBIHQ on a temporary duty (TDY) basis to address priority program needs. This program allows "field" Agents to bring "real world" experience to FBIHQ and to learn more about the "big picture" than is possible when working isolated cases. In FY 2004 alone, approximately 2,200 SAs benefitted from these TDY assignments.

24. A panelist participating in the 9/11 Commission's Public Discourse Project reported that the Bureau has 200 unfilled counterterrorism positions and is facing difficulty finding analysts and agents to fill those posts.

a. How many counterterrorism positions at the Bureau are presently unfilled? What are the obstacles to filling these positions?

Response:

As of 05/13/2005, there were approximately 202 vacant SA CT positions at FBIHQ. The primary obstacles to filling these positions, and positions at FBIHQ in general, are the recent spike in D.C.-area housing costs and the overall high cost of living in the Washington, D.C., area.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00096 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.037

The FBI's success in recruiting analysts has been better. The FBI's FY 2005 goal was to hire 880 analysts. As of 8/29/05, we had hired 660 new analysts (including both external hires and applications from qualified FBI employees serving in other positions). An additional 376 applicants have been selected and are being processed for employment, and 72 analyst candidates have been approved for employment but are not yet on board. During the same time period, 103 analysts have vacated analyst positions through reassignment, transfer to other federal agencies, resignation, or retirement. These numbers indicate that there are no particular obstacles to filling analyst positions, but there is some difficulty in keeping analysts on board.

b. What steps has the Bureau taken to fill these positions more rapidly?

Response:

To ensure a constant flow of applicants for all critical positions, the FBI attempts to publicize the rewards of FBI careers through various means, such as national advertising strategies targeting applicants with critical skills, including minorities, women, and persons with disabilities. These strategies include interactive campaigns and targeted advertisements in magazines, journals, television, radio, billboards, airports, newspapers, and theaters. The advertisements feature onboard employees who have critical experience and education that matches the FBI's targeted hiring objectives. This year's special effort to attract applicants to the analyst positions included a television ad that aired during the 2005 Super Bowl.

In addition, partnerships and networking vehicles have been developed to expand awareness of the FBI's career opportunities within the African-American, Asian-American, Hispanic, Native American, and Middle Eastern communities, and by addressing women's organizations and physically challenged audiences. The FBI has also developed partnerships with faith-based organizations to improve awareness of the FBI in those communities, and has implemented numerous internship programs in order to enhance the FBI's visibility and recruitment efforts at colleges and universities throughout the United States.

In addition to attracting and retaining critical employees through the increased use of the student loan repayment program and relocation and retention bonuses, the FBI has developed an FBIHQ Term Temporary Duty Pilot Program, pursuant to which SAs may apply for designated 18-month term FBIHQ assignments during a 90-day window. Selectees will receive FBIHQ supervisory credit and will be authorized to apply for field desks as SSAs after 15 months. As of 08/30/2005,

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00097 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.038

this pilot project had generated 567 applications for positions at FBIHQ and is expected to greatly reduce the staffing shortfall.

Similarly, a combination of methods is being employed to fill analyst positions quickly and to keep them filled. Recruitment bonuses totaling approximately $3.4 million were paid to approximately 380 analysts and retention allowances were afforded to two analysts in approximately the first 10 months of FY 2005 (many analysts are fairly new to the FBI and are not yet eligible for retention incentives). The availability of these bonuses is beneficial both because they encourage applicants to apply for analyst positions and because they encourage them to stay to complete the service to which they agree as part of the bonus offer. Retention has also been improved by our ability to increase access to the student loan repayment program, which also includes a service commitment. Whereas the availability of funds limited participation to 31 analysts during FY 2005, approximately 180 analysts participated in the student loan repayment program during FY 2005.

25. In July, John Perry, chief executive of CardSystems, testified before the House Financial Services Subcommittee on oversight and Investigations about a security breach that exposed as many as 40 million credit-card holders to potential fraud. Mr. Perry testified that CardSystems contacted the FBI about the data breach on May 23, but that the FBI took two days to respond, in part due to lack of clarity on the scope of the breach.

What is the FBI's policy on responding to reports of personal data security breaches, including how quickly agents should respond to such reports, and what expertise and forensic capabilities are available within the FBI to assess the scope of electronic data breaches?

Response:

With respect to the CardSystems Solutions, Inc. (CSSI) breach, we would like to note that the FBI initiated investigation on the day it was contacted based on information provided by the CSSI General Counsel to the FBI's Phoenix Division. At that point, CSSI had already determined that the intruder had been active within CSSI's network for nine months and CSSI had implemented defensive measures to mitigate further compromise. These measures included attempts to determine the type of data compromised and the extent of the breach, during which CSSI used the file transfer protocol to improperly retrieve from the intruder's computer the files that contained crucial transaction data and corresponding security codes obtained by the intruder through unauthorized queries. It was after this discovery that the FBI was notified, 8 days after CSSI noticed the unauthorized activity and 4 months after CSSI was alerted by the card

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00098 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.039

associations that they believed other unusual activity could be traced to a possible compromise of CSSI data.

As with all information of possible criminal activity received by the FBI, information relating to possible computer intrusions is initially evaluated to determine the appropriate course of action. The FBI's response depends on the circumstances involved: is there a possibility of loss of life, terrorist attack, state-sponsored intrusion placing the national information infrastructure at risk, prevention of criminal activity or further financial loss? (In the CSSI case, the FBI was advised that CSSI had implemented defensive measures to mitigate further compromise.)

The FBI's CyD includes the Special Technologies and Applications Section (STAS), which is often called upon by other FBI Divisions, USIC agencies, state and local governments, and foreign partners to determine the "who, what, why, when, where, and how" of computer intrusions. Through written reports, electronic disseminations, and other means, the STAS helps IAs, investigators, and decision makers understand what level of sophistication the activity represents, where evidence of the intrusion may be located, and, in some cases most importantly, what data was viewed, modified, added, deleted, or taken, and where it might reside thereafter. STAS is commonly called upon to re-live the electronic "day in the life of a computer file" to explain who saw it, "touched" it, moved it, and so on.

26. A June 2005 report by the Office of Inspector General evaluated DOJ's counter-terrorism task forces and advisory counsels, including 3 led by the FBI: the Joint Terrorism Task Forces (JTTFs), the National Joint Terrorism Task Force (NJTTF) and the Foreign Terrorist Tracking Task Force (FTTF).

a. The report found management and resources problems, including frequent turnover in leadership of the JTTFs, lack of counterterrorism expertise within the task force membership, as well as insufficient training, standards or orientation for members. What specific actions will the FBI undertake to address these concerns?

Response:

The FBI concurs with the findings of the DOJ Office of the Inspector General (OIG) regarding the importance of ensuring long-term, stable JTTF and Foreign Terrorist Tracking Task Force (FTTTF) leadership, effective and available training in critical substantive areas, and, in the case of the FTTTF, a settled location.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00099 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.040

All FBI investigators, in all programs, view the quality and completion of investigations as a priority. JTTF participants currently receive training in basic core functions, and training has been developed and delivered (in various formats) regarding the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, basic security issues (including the proper classification of intelligence communications), the roles, missions, and operations of the USIC, the FBI's ACS system, the Investigative Data Warehouse (IDW), the Threat Reporting System, and the tools, techniques, and skills needed to successfully investigate terrorism.

A recently created CTD Unit has been charged with assessing CT training and professional development needs, including those of the JTTFs. This Unit is developing a comprehensive NJTTF/JTTF Training Manual that will include the topics listed below. These topics will also be addressed in training provided to newly appointed JTTF members within their first year of service.

- Administration
- Security
- Automation/Computer Investigative Resources
- Introduction to Foreign Intelligence/Terrorism
- International/Domestic Terrorism Basic Courses (CD-ROM based training)
- Foreign CI Basic Course (CD-ROM based training)
- Surveillance Techniques
- Evidence Procedures
- Technical Writing
- Legal Training
- Asset/Source Recruitment and Management

The FTTTF has faced numerous challenges since its creation, and the pursuit of some of its own initiatives have been delayed while it provided critical support to the early efforts of the TSC, which was also recently created. The FTTTF has addressed the early problems created by fluid leadership and organizational structure, and has recently been relocated to "permanent" space, which will further improve stability. The FBI concurs with the OIG's recommendation that the FTTTF develop and implement a marketing plan to improve awareness and understanding of its services, and has taken steps to implement such a plan. The FTTTF's efforts to increase awareness of its role and responsibilities have included weekly briefings to visiting SACs and ASACs, participation in CTD's orientation program for new assignees, presentations to the NJTTF Conference, briefings to new SACs and Legal Attachés, and briefings to outside organizations (including the International Association of Chief of Police, National Sheriffs'

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00100 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.041

Association, Major City Chiefs, Interagency Intelligence Committee on Terrorism, and Homeland Security and Information Sharing Conference). In addition, the FTTTF has established a site on the FBI's Intranet, which will be replicated in part on the Secret Internet Protocol Router Network, and has published an Executive Guide to provide a concise synopsis of FTTTF capabilities and the means of requesting support.

b. In addition, the OIG report noted that the FBI has not signed Memorandums of Understanding (MOU) to define the roles, responsibilities, information sharing protocols and length of commitment with the agencies participating in these taskforces. When will the FBI have in place an MOU defining these critical elements?

Response:

Since 1980, the FBI has maintained Memoranda of Understanding (MOUs) with the state and local agencies that participate in the JTTFs. The FBI currently has in place 311 MOUs with agencies participating in the NJTTF and JTTFs, updated since 9/11/01 to incorporate such issues as polygraph requirements, information sharing policy, and length of commitment by individual participants. The FBI's CTD is currently working with DoD and DHS to standardize these MOUs and anticipates that the existing MOUs will be updated in the near future.

27. A recent report by the National Academy of Public Administration found that the FBI's information sharing practices are largely ad hoc with no mechanisms, such as penalties or incentives, to enforce or promote information sharing.

a. What progress has the FBI made in creating incentives to improve information sharing and penalties for failure to advance those goals?

b. What future actions does the FBI plan to improve its information sharing capabilities further?

Response to subparts a and b:

Please see our response to Question 6, above.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00101 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.042

28. In May of this year, it was reported that a search of IAFIS failed to identify the fingerprints of an individual detained by local authorities, Jeremy Jones, who was subsequently released and went on to kill three women and one teenage girl in three states. In addition, Mr. Jones is a person of interest in several other cases. An FBI official described the mistake as a "result of a technical database error, not a human examiner failing to make an appropriate match." What steps has the FBI taken to correct this database error and prevent a repeat of this type of mistake in the future?

Response:

The cause of the missed identification was a filter in the Automated Fingerprint Identification System (AFIS) component of the Integrated Automated Fingerprint Identification System (IAFIS). This filter, which was employed to narrow the field of records searched, erroneously eliminated Jones' record as a candidate because it was slightly outside the filter's parameters. When the FBI discovered this problem, it reviewed the need for the filter. Because of AFIS hardware upgrades completed in June 2004, it was determined that the filter was no longer necessary and should be disabled. This was accomplished on 1/9/05.

In addition to disabling the problematic filter, the FBI has taken several steps to ensure IAFIS' integrity. These steps have included an inspection of the system and the events that led to the missed identification, a search of the database to identify duplicate criminal history records, and the initiation of an aggressive program to detect and prevent missed IAFIS identifications. This program includes a quality assurance review of approximately ten percent of all transactions. In addition, because Jones used the exact name, date of birth, and social security number of another subject who was in prison at the time, causing additional confusion in making the identification, the FBI has initiated a review of all records that have exact matches of descriptive information to ensure they are not duplicate records and to provide investigative leads to law enforcement. Finally, the FBI has received funding for a 2006 effort to implement an overall enhancement of IAFIS that will involve substantial upgrades to the AFIS component. This broad enhancement was first conceptualized by the FBI, along with its law enforcement partners, in September 2003.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00102 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.043

29. The consolidated watchlist uses 4 risk-based handling codes to designate how law enforcement should respond when encountering individuals on the list. A recent Inspector General report found that nearly 32,000 "armed and dangerous" individuals are designated for the lowest handling code. This code does not require law enforcement encountering those individuals to contact the TSC or any other law enforcement agency. Some of these individuals were also described as "having engaged in terrorism," "likely to engage in terrorism if they enter the Untied States," "hijacker," "hostage taker," and "user of explosive or firearms." In press reports, the FBI has countered that legal restrictions prevent officers from ordering a suspect held without an arrest warrant or other evidence.

Notwithstanding strategic reasons or legal requirements that weigh against immediate detention of these individuals, there is a legitimate concern about designating such individuals for the lowest handling. You indicated at the July 27 hearing that you would look into the matter and respond.

a. Why are individuals described in such dangerous terms designated for the lowest handling?

b. Is there a code that would allow TSC to designate these individuals in such a way that law enforcement encountering them would be aware of the possible danger or use the opportunity to update TSC on any encounters with those individuals?

Response to subparts a and b:

Director Mueller provided this information to Senator Leahy by letter dated 8/1/05. A copy of that letter is attached as Enclosure D.

It is important to understand that Handling Codes (HCs) are not associated with threat levels; all terrorism-related entries in the Violent Gang and Terrorist Offender File (VGTOF) are assigned HCs, and the first line on the NCIC screen for all these entries advises: "Warning, approach with caution." The purpose of assigning the different HCs is to identify the government's authority to take legal action with respect to the individual based solely on the individual's inclusion in VGTOF. Encounters with some of the 9/11/01 hijackers shortly before those attacks taught us the importance of arresting, detaining, or otherwise appropriately responding when those who pose a terrorist threat are encountered. If a local law enforcement officer encounters an individual for whom there is a pending arrest warrant related to terrorism (HC1), the officer needs to know to effect an immediate arrest. Similarly, a law enforcement officer who encounters an individual of investigative interest with respect to terrorist activity (HC2) needs to know to detain that person to obtain more information. Clearly, these individuals may be equally dangerous, so the HC doesn't identify the degree of danger they

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00103 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.044

pose to the law enforcement officer (in fact, the HC1 may be based on a warrant related to "white collar" terrorism financing, while the HC2 may be based on facts indicating bomb construction, so an HC2 could, in fact, be more dangerous to the officer than an HC1). Instead, the HC indicates what response by law enforcement is lawful and appropriate (arrest, detention, or otherwise) based on the information available to the TSC. All HCs request TSC notification so the TSC can assist in coordinating the response, and all HCs are subject to revision based on new information or changes in status.

HCs, which identify the permissible response if an individual is encountered, are unrelated to Immigration and Nationality Act (INA) codes, which are assigned by DHS to identify the nature of the derogatory information on an individual. We defer to DHS with respect to the assignment and use of INA codes.

30. The OIG Report found that there is "no formal strategic plan" to guide the [Terrorist Screening] Center's progress, staffing, structure and future planning, but that such a plan would assist the TSC in addressing the most significant weaknesses identified in the OIG report. In addition, the Report noted that TSC has no formal procedure for evaluating its own performance. When will the TSC develop a formal strategic plan or procedures for performance evaluation?

Response:

The TSC's formal strategic plan, dated 6/17/05, addresses the organization, structure, and progress of the TSC, including new initiatives, plan implementation, and progress reviews. The TSC's performance will be evaluated according to metrics designed to assess the quality of TSC data and its contribution to the performance and effectiveness of TSC customers. TSC will develop a means of using metrics to evaluate TSC performance over time, and each review will be assigned an owner, priority, start date, and projected end date.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00104 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.045

31. In May 2005, the Government Accountability Office issued a report on U.S. passport fraud detection efforts and identified several weaknesses in those efforts, including that TSC neither provides consolidated terrorist watch list information to the State Department in a systematic manner nor routinely provides the names of other individuals wanted by federal and state law enforcement authorities. The Report indicated that the State Department sent a proposal on sharing watchlist information to TSC in January of 2005 and a written request outlining its needs for access to information on wanted persons in April 2005.

a. What steps has TSC taken to share with the State Department information from the consolidated watchlist and the FBI's database on wanted persons?

Response:

An MOU between the Department of State (DOS) and the TSC regarding the export of TSC data into the Passport Class System was signed by Assistant Secretary of State for Consular Affairs Maura Harty and by TSC Director Donna Bucella in late June 2005. The program was implemented on 7/25/05.

The FBI's database on "wanted persons" is managed by the FBI's CJIS Division, rather than by the TSC. In June 2005, the FBI began providing to DOS all NCIC "wanted persons" information derived from FBI files in order to enhance passport screening and fugitive apprehension. The FBI and DOS are in the process of completing an MOU to document this process. In addition, the FBI and DOS are attempting to coordinate the provision of access to non-FBI "wanted person" information in NCIC for passport screening purposes.

b. What, if any, obstacles prevent sharing this information, and when will the State Department have access to this information?

Response:

There are no obstacles to the sharing of this information. The TSC has been exporting Terrorist Screening Database (TSDB) data to DOS since the program was implemented on 7/25/05.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00105 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.046

32. What is the average amount of time it takes to translate high priority counter-intelligence audio, which the Inspector General found is not always reviewed within 24 hours?

Response:

At present, the FBI does not collect this information. Based on the OIG report, we are conducting a complete review of our collection of language processing management data to ensure we capture this and other vital information.

33. I understand from your colleagues in the Bureau that real time translation is likely not possible, but they often speak of "near real time." Translating material on a near simultaneous basis could be critical to preventing an attack, just like listening to suspected criminals on a traditional wiretap can help officials to prevent planned crimes from being carried out. What are the realistic prospects for such material to be translated in something approximating real time?

Response:

Given the volume, velocity, and variety of information collected, near real-time translation of material is not likely absent advances in machine translation capabilities. Near real-time review of critical language material is possible through a combination of priority setting, selection tools, and rudimentary machine translation capabilities.

The FBI is not focused on moving from "near real time" review to "real time" review because it is far more efficient for a linguist to review the foreign language material after it has been recorded. The linguist is able to eliminate any "down time" (such as "dead air" time) by scanning the audio or text rather than listening to or reading the material as it is being produced. In addition, review is conducted in "near real time" because foreign language material is most often routed to the linguist electronically, typically as soon as the phone call or other event ends. Routing the work to the linguist, as opposed to sending the linguist to the collection site, allows the FBI to address even obscure languages quickly and enables a single linguist to process the work from several offices. This would not be possible if we were to place linguists physically at the site of collection to process material in "real time." "Near real time" may be as soon as the target hangs up the phone or up to 24 hours later, depending on the availability of resources proficient in the foreign language.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00106 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.047

34. Your testimony states that the FBI can generally translate its high priority counter-terrorism audio within 24 hours. When the FBI misses that 24 hour target, what is average amount of time that it takes to translate high priority counter-terrorism material?

Response:

The FBI endeavors to review all of its highest priority Foreign Intelligence Surveillance Act (FISA) material within 24 hours of receipt and is generally successful in doing so. The OIG recently conducted tests in eight of the FBI's major translation centers and did find two instances in which material from the highest priority cases was not reviewed within 24 hours (a third instance noted by the OIG involved a negligible amount of material), but in both cases the material was reviewed within 48 hours.

35. The FBI modified its quality control guidelines in response to the July 2004 audit by the Inspector General. Those new guidelines took effect in December 2004. The July OIG report shows, however, that there is still no nationwide system in place to ensure that FBI field offices perform quality control reviews, or that they monitor the results of reviews. How can you explain this delay?

Response:

At the time of the OIG report, our quality control program had just been implemented and the first reports from that program were not available for OIG review. The OIG did acknowledge that after auditors had completed their field work the FBI provided "documentation showing that it had initiated a nation-wide tracking system and had used the new system to track the first quarterly report received in April 2005." The FBI continues to improve this program and expects to make further progress as we are able to hire and deploy additional personnel. These additional personnel resources will include Regional Program Managers and linguists, who will assist in improving quality control measures and in monitoring the field's compliance with these measures and with other foreign language program initiatives.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00107 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.048

Questions Posed by Senator Feingold

36. Thank you for the additional information your office provided regarding the FBI's use of commercial data. When we met earlier this month, you told me that the FBI has contracts with commercial data brokers, but that agents search these databases only for particular information about individuals already under suspicion, and not to look for patterns of behavior that indicate an individual might be a terrorist. Is that a fair characterization?

Response:

That is generally a fair characterization. Commercial databases can be searched by FBI employees for information about individuals and groups in whom the FBI has a valid investigative interest. The FBI does not search commercial databases for patterns of behavior that might be associated with actions of terrorists.

37. Please provide the Committee with copies of the contracts that the FBI has entered into with commercial data brokers.

Response:

By letter to the Committee dated 4/18/05, we responded to a 3/31/05 letter requesting documents, including active FBI contracts with data brokers. In our response, we noted that on 4/7/05 Judiciary Committee staff received a detailed classified briefing on contracts DOJ and the General Services Administration (GSA) have with data brokers to obtain personal information for investigative purposes. Committee staff also received an unclassified briefing on 3/21/05 from DOJ and FBI officials regarding a recent ChoicePoint compromise, a portion of which addressed DOJ contracts with data brokers. As discussed during the 4/7/05 briefing, the FBI uses the services of Axciom, ChoicePoint, Dun and Bradstreet, iMAPdata, LexisNexis, Seisent (Accurint product), and Westlaw through contracts held by DOJ, GSA, and the Department of the Interior. DOJ provided to the Committee redacted copies of relevant DOJ contracts during the week of 4/11/05.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00108 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.049

38. If the FBI begins to explore the application of data mining technology to commercial data, will you commit to informing the Committee about your plans?

Response:

As the FBI has indicated in previous written responses to this Committee, the FBI does not use public source providers to data mine or run "open-ended" searches for people who might fit a certain pattern. If the FBI should decide to run "open-ended" pattern searches, we will notify the Committee.

39. Please provide information, in classified form if necessary, regarding any reliance by the FBI on the use of pattern analysis technology or other statistical methods to analyze its own investigative files. Please detail the type of technology employed, the type of data subject to such analysis, any outside contractors involved in this type of analysis, and any guidelines governing such analysis.

Response:

If the term "pattern analysis technology" is used to mean the ability to enter into a computer system a series of general characteristics that operates over a broad set of data to automatically provide a list of those likely to be terrorists, the FBI neither has such a capability nor is seeking to develop one. The FBI does, however, use the IDW to conduct ad hoc and batch queries across documents stored as unstructured data (approximately 50 million documents stored in "flat files," which have no significant structure to permit the identification of data elements) and structured data (approximately 413 million documents containing structure that reveals data elements and permits extraction, transformation, and loading into a database). The set of searchable documents is growing through the addition of new sources of information from both FBI systems and those of other Federal organizations.

These capabilities are provided by commercial products that are integrated into IDW to provide search services, name processing services, and extraction, transformation, and loading services.

Search services.

Search services provided by Chiliad products operate over "unstructured" documents (such as text-rich messages, scanned documents, word processing files, and PowerPoint files), and over data extracted and loaded into Oracle databases. The Chiliad product will operate over data in any Open DataBase

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00109 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.050

Connectivity-compliant relational database management system. Data fusion takes place during indexing and search/analysis. The Chiliad technology suite uses various pattern matching techniques, including contextual searches, probabilistic searches, automatic concept recognition, named entity extraction, and a stemming algorithm.

Search services provided by Convera use Adaptive Pattern Recognition. Processing technology. This technology allows investigators to perform searches for people who have aliases, name variants, or a variety of name spellings, and permits complex searches with complete flexibility in search terms, including any number of wildcards or patterns. Convera also permits the application of pattern recognition technology to search profiling. This technology allows users to register queries using a pattern recognition format, after which all new content flowing into the system is examined for matching patterns and/or wildcards in real-time and users are notified of matches.

Name processing services.

Applications provided by Language Analysis Systems are used to compute probabilities and associated confidence factors for male/female sex determination based on name, to compute probability that a given name is associated with each of 12 nationality groups, and to identify a set of closest matching names in an existing database of names. The computations of probable gender, nationality group, and closest matching names are achieved using pattern matching and statistical analyses of names based on extensive research and analysis of the linguistic and computational properties of names.

Extraction, transformation, and loading services.

IQ Insight is a data profiling tool that can be used to query database tables or flat files to identify patterns, including user-defined patterns (e.g., phone numbers, social security numbers, electronic mail message addresses, names, titles, company names and departments, dates, and addresses). IQ Insight is used to verify that the information in a particular field meets the range, format, and other characteristics expected for that information.

Several contractors assist with IDW maintenance: Scientific Applications International Corporation, Northrop Grumman Corporation - Information Technology Division, and Titan Systems Corporation assist with system operations and maintenance; Chiliad, Convera Corporation, and Informatica Corporation provide vendor support; EW Solutions, Mitretek Systems, and

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00110 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.051

Buchanan Edwards assist with security and data engineering; and SPAWAR, Eagan, McAllister Associates, Inc., provide program management support.

IDW is an FBI system, and all users must complete mandatory FBI Information Technology Security Awareness training. Users include FBI SAs and analysts, contract analysts serving in operational capacities, and detailees from other federal, state, and local agencies who have been verified as having an operational need for access. Multiple banners (FBI network and IDW) alert users to the restrictions on their use of the IDW system.

Requests to add data sources to IDW must include Privacy Impact Assessments (PIAs), which are reviewed by the FBI Office of the General Counsel (OGC). OGC's reviews of IDW PIAs are then reviewed by the FBI Information Policy Sharing Group, which must approve all sources of data hosted by IDW.

40. The Patriot Act authorized roving taps under the Foreign Intelligence Surveillance Act. That provision did not include an ascertainment requirement, as there is for roving taps under the criminal law. The criminal wiretap statute requires that for roving taps, "the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted." 18 U.S.C. § 2518(11)(b)(iv). This ensures that when the order itself does not specify the facility to be tapped, innocent people's phone and computer conversations are not intercepted.

a. Would you object to including a similar ascertainment requirement for FISA roving taps? If your answer is "yes," please explain your reason(s).

Response:

As explained in more detail in the 5/24/05 letter to the Senate Select Committee on Intelligence attached as Enclosure E, the FBI would object to imposing that "ascertainment requirement" for FISA roving wiretaps. The proposed ascertainment requirement would deprive FBI investigators of necessary flexibility in conducting Section 206 roving surveillance. Targets of FISA surveillance are often among the most well-trained and sophisticated terrorists and spies in the world, and are capable of engaging in detailed and extensive counter-surveillance measures. Adding the proposed ascertainment requirement might jeopardize the FBI's ability to conduct surveillance because, in attempting to physically ascertain where the target communication will take place, FBI agents would run the risk of being exposed to sophisticated counter-intelligence efforts.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00111 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.052

In addition, the proposed ascertainment requirement would impose significant, unwarranted burdens in cases that are already difficult because of actions by the target that have the effect of thwarting the surveillance. Generally, communications intercepted by criminal Title III surveillance are monitored and minimized contemporaneously by law enforcement personnel. In contrast, communications intercepted pursuant to FISA are generally not contemporaneously monitored. FISA surveillance generally involves after-the-fact review pursuant to minimization procedures approved by the FISA Court (FISC) that limit the acquisition, retention, and dissemination of information about United States persons (thus protecting the privacy of innocent individuals). Under FISA, regardless of whether the surveillance is pursuant to a section 206 order, conversations of "innocent people" are minimized (i.e., not retained in any easily retrievable manner), unless they are talking to or about the authorized target of the surveillance.

Presently, Section 206, together with the practicalities of how surveillance occurs (as discussed below), provides sufficient safeguards to ensure that an innocent person's telephone and computer conversations are not inadvertently intercepted. The target of the roving surveillance must be identified or described in the FISA application with sufficient particularity to permit the FISC to conclude that there is probable cause to believe the target is a foreign power or an agent of a foreign power. Section 206 roving surveillance can be ordered only if the FISC finds, after having determined that the requirements for FISA electronic surveillance have been met, that the actions of the specified target may have the effect of thwarting the surveillance. If the government can demonstrate that to the satisfaction of the FISC, it then obtains a secondary order that can be served on any provider of a facility subsequently determined to be used by the target. As a practical matter, the FBI determines that the target is using a particular facility before it serves the order and begins monitoring the new facility. That determination is, however, very different from a requirement that the FBI must have observed the target near to or on the new facility before it can monitor the resulting communication.

b. Please explain, in the context of a FISA roving tap, how agents make the decision which facilities to tap. If agents do not ascertain that the target is using a particular facility, how do they decide which facility to tap? How do they decide when to start listening in on the tap?

Response:

This question suggests that there may be a misapprehension about how "roving FISA surveillance" under Section 206 is conducted.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00112 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.053

When the FBI determines that the target's actions may have the effect of thwarting surveillance (either by virtue of the target's own practice of switching providers or because the target works for an entity that has an established practice of engaging in tradecraft that thwarts surveillance), the FBI may apply for "roving" electronic surveillance authority. In that event, the court's order would require the known telephone service provider to facilitate the surveillance and would provide the FBI with another order that requires a "specified person" to facilitate the surveillance of the target. The FBI can then serve that second order on any cellular telephone service provider after the FBI has confirmed that the target is using or about to use a new facility, i.e., that he has "roved." Currently, a notice is filed with the FISC identifying the new facility after an order is served on the new provider.

41. Do you agree that if Congress were to grant the FBI the administrative subpoena authority that you sought at the hearing, the FBI would be highly unlikely to seek a Section 215 order or a National Security Letter ever again? If your answer is no, please describe the circumstances under which the FBI would seek a Section 215 order or an NSL rather than issue an administrative subpoena.

Response:

We do not agree that obtaining administrative subpoena authority would render section 215 orders or National Security Letters (NSLs) obsolete. Generally, the FBI will use the most effective and time-efficient tool available for an investigation, taking into account the type of record sought and our knowledge of the custodian of those records. Administrative subpoena authority would clearly provide a mechanism for obtaining relevant information in national security investigations quickly and without significant expenditure of personnel resources. Although administrative subpoenas might well become the FBI's national security tool of choice, they would not become its only tool. For example, the FBI may well choose to seek a Section 215 order in a very sensitive investigation in which the added imprimatur of a court order to maintain the secrecy of the order is needed (e.g., past experience with the document custodian suggests a lack of care with administrative requests). The FBI may also use a 215 order if it is seeking records that are particularly sensitive, making review by a court before seeking the documents appropriate. The FBI's experience with criminal administrative subpoenas shows that criminal investigators do not limit themselves to one tool, but instead use whatever tool most effectively and efficiently obtains the needed information. We expect our SAs handling national security investigations to exhibit the same initiative in their investigations.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00113 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.054

42. Thank you for your prior responses to questions about the operations of the Terrorist Screening Center (TSC). You explained in those responses that TSC has hired a Privacy Officer to help address complaints about the operation of the TSC watch lists. Please explain the role of the Privacy Officer. Who does the Privacy Officer report to? Does the Privacy Officer have full clearance to review all TSC data?

Response:

The TSC Privacy Officer is formally supervised by the TSC Director, and additionally reports informally to the TSC Chief of Staff to ensure proper coordination of assignments and other matters. The Privacy Officer is responsible for establishing internal policies and procedures to ensure the TSC is in compliance with laws and policies related to the handling of personal information, and for recommending additional policies to ensure that appropriate privacy protections are afforded even in the absence of regulation. The Privacy Officer has full clearance to access all data maintained and used by the TSC in the performance of its mission.

43. The June Inspector General report evaluating TSC identified problems with the completeness and accuracy of the watch list data, in terms of both omitting known terrorists and including inaccurate information about individuals. What steps is the TSC taking to rectify this problem?

Response:

The TSC is using sophisticated database queries to check for data anomalies, performing record-by-record reviews of the data known to be the most likely to contain inaccuracies, and employing sophisticated custom software to evaluate incoming data against 44 business rules in order to ensure errors do not enter the database.

44. Would the FBI be willing to allow cleared staff of the Judiciary Committee to visit the TSC to better understand how the watch list process works, how names are added and removed from the list, and how TSC interacts with other agencies?

Response:

On various occasions, the FBI has invited Judiciary Committee members and staff to tour the TSC and obtain a briefing concerning its activities and evolution. We would be pleased to arrange such a visit at the Committee's convenience.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00114 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.055

45. Please provide a list of each federal government agency, department or other entity that relies on the TSC to screen individuals, and the purpose of each screening program. Please include programs in which the government agencies run the names of private sector employees against the watch list.

Response:

The law enforcement components of federal agencies rely on the TSC to screen individuals through the TSDB to identify known or appropriately suspected terrorists, and to provide this information to them on a real-time basis. The initial inquiry by federal law enforcement officials is most often precipitated by a "hit" in the NCIC's VGTOF. The majority of federal encounters in which the TSC is engaged are initiated by the National Targeting Center, which is managed by DHS.

The TSC does not currently run the names of "private sector employees" against the watchlist or any other TSC database unless, of course, they are the subjects of the law enforcement encounters described above. The establishment of programs to support private sector screening is a task for which the DHS is responsible. When those programs are established, the TSC will provide appropriate mechanisms to ensure these screening opportunities are managed properly.

46. Please provide information about the state and local agencies, departments or other entities that rely on the TSC to screen individuals, and the purposes for which they do so.

Response:

All state and local law enforcement agencies with NCIC access rely on the TSC's TSDB and the NCIC system to identify potential terrorism subjects.

The TSC is a multi-agency organization established under the authority of Homeland Security Presidential Directive 6 to ensure that the names of known or suspected terrorists collected by various U.S. Government agencies are merged into one consolidated list and appropriately shared with federal, state, local, territorial, tribal, and consular authorities, as well as with certain foreign governments. Participants in the TSC include the ODNI, DOJ, DHS, DOS, DoE, and Department of the Treasury. TSDB information is exported to multiple supported systems, including the NCIC's VGTOF. State and local law enforcement authorities are able to query VGTOF for operational direction concerning positively identified known or appropriately suspected terrorists on a "real-time" basis. The FBI's Terrorist Screening Operations Unit (TSOU)

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00115 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.056

coordinates the operational and investigative response to these inquiries with the appropriate JTTF, which includes representatives from the intelligence community and from the federal, state, and local law enforcement communities. The JTTF conducts liaison with the encountering agency. The TSC also notifies the North American Aerospace Defense Command (NORAD) and the Federal Air Marshal Service (FAMS) of positive encounters during TSC's airline screening process. NORAD is alerted to this information to provide them an opportunity to monitor "Selectee Flights," and FAMS is alerted to permit them to schedule Air Marshals on all "Selectee Flights," making better use of limited resources. These processes have been developed to address gaps within the overall terrorist screening effort and to improve the flow of terrorism-related information.

The ability of the TSC to identify, collect, review, and analyze intelligence from encounters with known or appropriately suspected terrorists increases the effectiveness of the FBI's overall terrorism intelligence base. Daily, this information is shared by the TSC's Tactical Analysis Unit with the FBI's FIGs, which include representatives from the FBI field offices in which they reside and may also include representatives from intelligence agencies and federal, state, and local law enforcement agencies. Through these efforts and those noted above, the TSC has assisted in greatly improving the flow of information between the FBI and state and local law enforcement agencies.

47. There have been reports that FBI agents registered serious concerns about interrogation techniques they witnessed officials from other agencies or departments employing at Guantanamo Bay.

a. When were these concerns brought to your attention?

Response:

Director Mueller does not have a specific recollection as to when he first received this information, but believes that by early 2002 he had determined that FBI Agents participating in interviews overseas should follow FBI protocols.

b. What steps has the FBI taken within the Administration to oppose the use of coercive interrogations?

Response:

The FBI has clearly communicated its view that rapport-building interview techniques are more effective than coercive or other aggressive techniques.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00116 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.057

ENCLOSURE A

QUESTION 11b

SENTINEL STATEMENT OF WORK

46051.058

UNCLASSIFIED
FOR OFFICIAL USE ONLY

Version 2.1
5 Aug 2005

SENTINEL
STATEMENT OF WORK

FOR OFFICIAL USE ONLY
UNCLASSIFIED

46051.059

SOW To Be Determined (TBD)/To Be Reviewed (TBR)/To Be Supplied (TBS) Table

Seetion	TBD/TBR/TBS	Closnre Plan
5.5.3	Identify the number of training locations.	Offeror closes with proposal submission (based on the proposed training approach).
8	Contractor to provide base period length, Phase durations and end date as part of the proposal.	Offeror closes with proposal submission.
9.1-1, 18.81	**Delivery Acceptance Review deliverable 9.1-1**	Offeror closes with proposal submission.
9.2	Contractor to supply CLIN durations and start and end dates as part of the proposal.	Offeror closes with proposal submission.
11.3	Need date for test data	Offeror closes with proposal submission.
15.5.1	Usability Standards	Offeror closes with proposal submission.
15.7	Workspace -number of spaces to be determined.	Offeror closes with proposal submission.

TABLE OF CONTENTS

1. ACQUISITION **6**

2. BACKGROUND AND OBJECTIVES **6**
2.1 Background 6
2.2 SENTINEL Acquisition Objectives 6

3. APPLICABLE DOCUMENTS **8**
3.1 Compliance Documents 8
3.2 Guidance Documents 8

4. SCOPE **8**

5. SPECIFIC TASKS **9**
5.1 Task 1-Contract-Level and Task Order (TO) Management 11
5.1.1 Task 1 Subtask 1-Contract-Level Program Management 11
5.1.2 Task 1 Subtask 2-Task Order Management 11
5.1.2.1 Earned Value Management System (EVMS) Implementation 11
5.1.2.2 Risk Management Program 12
5.1.2.3 Configuration Management (CM) Program 12
5.1.2.4 Quality Assurance (QA) Program 12
5.1.2.5 Security Management (facilities and personnel) 12
5.1.3 Task 1 Subtask 3-Data Management Program 12
5.1.4 Task 1 Subtask 4-In Progress Review Support 13
5.1.5 Task 1 Control Gates and Program Reviews 13
5.1.6 Task 1 Deliverables 13
5.2 Task 2-SENTINEL Systems Engineering and Architecture 13
5.2.1 Task 2 Subtask 1-SENTINEL Systems Engineering Management 13
5.2.2 Task 2 Subtask 2-SENTINEL Architecture Management 15
5.2.3 Task 2 Control Gates and Program Reviews 15
5.2.4 Task 2 Deliverables 16
5.3 Task 3-Phase Design, Development, Test, Implementation, and Integration 16
5.3.1 Task 3 Subtask 1-Phase Design 16
5.3.2 Task 3 Subtask 2 Phase Development and Test 17
5.3.3 Task 3 Subtask 3-Phase Implementation and Integration 17
5.3.4 Task 3 Subtask 4-Operations and Maintenance Support 17
5.3.5 Task 3 Control Gates and Program Reviews 18
5.3.6 Task 3 Deliverables 18
5.4 Task 4-IT Operations and Maintenance 18
5.4.1 Task 4 Subtask 1-Pre-Full Operational Capability (FOC) Operations and Maintenance (separately priced options for O&M of each Phase) 20
5.4.1.1 Conduct System Administrator Training 20
5.4.1.2 Conduct of Pre-FOC Operations and Maintenance 20
5.4.2 Task 4 Subtask 2-Operations and Maintenance Transition (separately priced option) 21
5.4.2.1 Conduct System Administrator Training 21
5.4.2.2 Conduct Operations and Maintenance 21
5.4.3 Task 4 Subtask 3 Post-FOC Operations and Maintenance and Sustainment (separately priced options for two one-year periods) 21
5.4.3.1 Conduct System Administrator Training 21
5.4.3.2 Conduct Operations and Maintenance 22
5.4.4 Task 4 Control Gates and Program Reviews 22
5.4.5 Task 4 Deliverables 22
5.5 Task 5-Organizational Change Management 23
5.5.1 Task 5 Subtask 1-Assess and Plan Change Management 23
5.5.2 Task 5 Subtask 2-Develop Training Material 23

5.5.2.1 Training Strategy and Plan ... *23*
5.5.2.2 Training Media ... *24*
5.5.2.3 Technology-Based Training ... *24*
5.5.3 Task 5 Subtask 3-Conduct User Training ... *24*
5.5.4 Task 5 Subtask 5-Continued User Support ... *24*
5.5.5 Task 5 Subtask 6-Extended Support ... *24*
5.5.6 Task 5 Subtask 7-Support to Government Communications ... *24*
5.5.7 Task 5 Control Gates and Program Reviews ... *25*
5.5.8 Task 5 Deliverables ... *25*

6. CONTRACT TYPE ... **26**

7. PLACE OF PERFORMANCE ... **26**

8. PERIOD OF PERFORMANCE ... **26**

9. DELIVERABLES/DELIVERY SCHEDULE ... **26**
9.1 Data Requirements ... 26
Table 9.1-1 Task Order Data Requirements ... *27*
9.2 Task Order Delivery Schedule (TBR) ... 29

10. SECURITY ... **33**
10.1 Personnel and Facility Clearance Requirements ... 33
10.1.1 Personnel Requirements ... *33*
10.1.2 Facility Security Requirements ... *33*
10.2 Security Acquisition Section Requirements ... 34
10.2.1 Access to Classified Information ... *34*
10.2.2 Products that Provide or Include Software and/or Hardware ... *36*
10.2.3 Use of an Information Technology System to Support Contract Performance ... *37*
10.2.4 Virus Control ... *37*
10.2.5 Contracting Officer's Security Representative ... *38*

11. GOVERNMENT FURNISHED EQUIPMENT (GFE)/GOVERNMENT FURNISHED INFORMATION (GFI) ... **38**
11.1 Inventory Requirements ... 38
11.2 Government Furnished Equipment ... 38
11.3 Government Furnished Information: ... 39

12. PACKAGING, PACKING, AND SHIPPING INSTRUCTIONS ... **39**

13. INSPECTION AND ACCEPTANCE CRITERIA ... **40**

14. ACCOUNTING AND APPROPRIATION DATA ... **40**

15. OTHER PERTINENT INFORMATION OR SPECIAL CONSIDERATIONS ... **40**
15.1 Performance Criteria ... 40
15.2 Organizational Conflict of Interest (OCI) Mitigation Plans ... 44
15.3 Reserve ... 45
15.4 Contractor Travel ... 45
15.5 SENTINEL Standards ... 45
15.5.1 Usability Standards (TBR): ... *45*
15.5.2 Development Standards: ... *45*
15.5.3 Operations and Maintenance Standards ... *45*
15.6 Government Space at Contractor Facility ... 46
15.7 Installation Support ... 47
15.8 Key Personnel ... 47
15.9 Software Licenses ... 47
15.10 Development Environment ... 47

15.11 Applets, Plug-ins and Other Applications Planned for FBINet 47
15.12 Software Engineering Institute (SEI™) Capability Maturity Model Integration (CMMI®) Level 3 Requirement 48
15.13 Vendor Contracts for Operations and Maintenance 48
15.14 Mandatory Patch Management Procedures 48
15.15 Release Information – Publications by Contractor Personnel 48
15.16 Privacy Act 49

16. POST-AWARD ADMINISTRATION 49

17. EVALUATION CRITERIA 50

18. DATA ITEM DESCRIPTIONS 54

Attachment 1-Earned Value Management System Requirements

Attachment 2-SENTINEL DD FORM 254

Attachment 3-Data Delivery Schedule

Attachment 4-Key Personnel-Duties and Qualifications

Attachment 5-Communications Strategy and Action Plan

Attachment 6-Training Strategy and Plan

Attachment 7-SENTINEL Stakeholder and Organizational Risk Assessment

Attachment 8-Organizational Impact Assessment

Attachment 9-Workforce Transformation Strategy and Plan

Attachment 10- Training Administration Report

Attachment 11- Award Fee Plan

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00122 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.083

1. Acquisition

This Statement of Work (SOW) describes the Federal Bureau of Investigation's (FBI's) requirements for SENTINEL. The contractor shall be responsible for furnishing all personnel, facilities, equipment, material, supplies, support and management and shall perform all functions necessary to design, develop, integrate, test, deploy, operate and maintain SENTINEL as set forth in the SOW and the SENTINEL System Requirements Specification (SRS). This SOW is intended for use with the documentation listed in SOW Section 3.0, Applicable Documents. All of the requirements in the SRS, whether specifically referenced or not in the SOW, shall apply to the contractor's deliverable services and service performance.

2. Background and Objectives

2.1 Background

The Federal Bureau of Investigation (FBI) is completing the building and deployment of several infrastructure systems that modernize its IT capabilities. Referred to as the Trilogy Program, this FBI initiative consists of the following interrelated components:

- The Information Presentation Component (IPC) encompasses hardware and software within each office to provide each employee with a current desktop environment and equipment.
- The Transportation Network Component (TNC) is composed of high-speed connections linking the offices of the FBI.
- The User Applications Component (UAC) will include SENTINEL enhancing each employee's ability to access, organize, and analyze information.
- The Enterprise Operations Center (EOC) is the FBI's infrastructure management center that oversees, monitors, and manages the Trilogy assets.

The IPC, TNC and EOC efforts are complete. The operational system is referred to as FBINet.

The FBI currently uses paper as their system of record while electronically managing the information. The current methods of managing case file information are outdated and inefficient. In order for the FBI to more effectively perform its mission, the case management system must be upgraded to utilize enabling information technologies.

SENTINEL will transform the way the FBI does business, allowing the Bureau to move from a primarily paper-based case management system to an electronic system of records. SENTINEL will leverage technology to reduce redundancy, eliminate bottlenecks and inefficiencies, and maximize the FBI's ability to use the information in its possession. SENTINEL will be an integrated system that will support the processing, storage, and management of information to allow the FBI to more effectively perform its investigative and intelligence operations.

The SENTINEL acquisition continues the FBI's transformation to an enterprise-wide automated case management system that began with the Virtual Case File (VCF) Pilot.

2.2 SENTINEL Acquisition Objectives

The objectives of the SENTINEL acquisition are:

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00123 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.064

- Objective 1: To incrementally design, develop, integrate, test, and implement a set of capabilities that meets the requirements outlined in the SENTINEL System Requirements Specification with operationally useful increments delivered approximately every 12 months. At a high level the delivered system shall:
    - Implement paperless case management and workflow capability (Priority 1).
    - Provide a single point of entry for investigative case management.
    - Implement electronic records management.
    - Implement a new and improved Bureau-wide global index for persons, organizations, places, things, and events.
    - Facilitate information sharing among law enforcement agencies and the intelligence community.

- Objective 2: To efficiently and cost effectively transition users and data to the new system. Transition steps include:
    - Retiring FBI legacy case management systems (or elements of them) as rapidly and efficiently as possible.
    - Timely, accurate and efficient data migration from legacy systems.
    - Transition of all users to the new system as services and data become available.

- Objective 3: To establish an Organizational Change Management (OCM) strategy enabling users to learn new behaviors, skills, and business processes through robust training and outreach programs.

- Objective 4: To enhance user interaction with SENTINEL, combining new and legacy components through intuitive human system interfaces presenting actionable data and items of interest to the user as requested or via data rules.

- Objective 5: To provide the FBI with a flexible and extensible IT infrastructure for SENTINEL that accommodates incremental composition and integration of capabilities that achieve an event driven Service Oriented Architecture (SOA).

- Objective 6: To exploit and utilize to the maximum extent possible government owned and/or commercial-off-the-shelf (GOTS/COTS) components. The Government desires a modular, component-based approach leveraging standards-based protocols and the best of commercially available IT technologies.

- Objective 7: To successfully accredit each Phase beginning with the first deployment including:
    - Information assurance Approval to Operate at the level specified in the SRS
    - Recordkeeping certification and Approval to Operate as applicable to each Phase

- Objective 8: To operate and maintain each deployed Phase at the levels specified in the Government approved[1] contractor generated Service Level Agreements (SLAs).

[1] The Service Level Agreement will be generated as part of the Phase development activity by the contractor. The Government is the approval authority.

- Objective 9: To transition operations and maintenance of the system to the FBI's Information Technology Operations Division (ITOD) at the completion of the final operations and maintenance period (approximately two years after the final Phase deployment) or earlier at the request of the Government.

3. Applicable Documents

A list of documents referenced throughout the SOW is presented in sections 3.1 and 3.2. Compliance documents shall be complied with. Guidance documents are provided for reference.

3.1 Compliance Documents

a) FBI SENTINEL Configuration Management Plan V1.1, 20 July 2005
b) FBI SENTINEL Risk Management Plan V1.2, 8 July 2005
c) FBI Information Technology (IT) Life Cycle Management Directive (LCMD) Version 3.0 draft as of 30 June 2005
d) FBI SENTINEL System Requirements Specification (SRS) V1.1, 29 July 2005
e) FBI Certification and Accreditation Handbook V2.1, 1 Jun 05
f) National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M 1995, with Changes 1 (1997) and 2 (2001)
g) FBI Electronic Recordkeeping Certification Manual V1.0, 30 April 2004
h) NDIA PMSC Surveillance Guide - ANSI/EIA Standard 748 (current version at time of solicitation)
i) NDIA PMSC Internet Guide - ANSI/EIA Standard 748 (current version at time of solicitation)
j) Commercial Delivery Instructions J. Edgar Hoover (JEH) FBI Building and Washington Field Office (WFO) dated 27 Dec 2000
k) ITOD Data Unit, Equipment Installation Standards, 10 May 2005
l) ITOD Data Unit, Equipment Installation Standards (Clarksburg, West Virginia), 12 May 2005
m) Software Update Services (SUS) Patch Management Process, 20 April 2005
n) FBI SENTINEL Incremental Development Plan V1.0, 29 July 2005
o) FBI SENTINEL CONOPS, 25 July 2005
p) FBI Enterprise Architecture (EA) Target Architecture Report V1.0, 31 May 2005
q) FBI SENTINEL Test and Evaluation Master Plan (TEMP) V1.1, 22 July 2005

3.2 Guidance Documents

a) FBI SENTINEL Program Management Plan V1.0, 22 July 2005
b) Technical Reference Model, V 0.51, 1 July 2005
c) Oracle Database Element Naming Standards V1.1, 24 September 2001
d) Oracle Database Development Standards, Version 1.0, 14 April 2003
e) Oracle Database Security Marking Standards V1.0, 26 March 2002
f) Oracle Database User Audit Requirements Specification, Version 1.3, 28 Sep 2001

4. Scope

The task order scope is worldwide and includes efforts related to four CIO-SPi-2 Task Areas as follows:

- CIO-SP2i Task Area 3. IT Operations and Maintenance. (Objectives 8 and 9 above)
- CIO-SP2i Task Area 4. Integration Services (Objectives 1, 2, 3, 4, 5, 6, and 7 above)
- CIO-SP2i Task Area 5. Critical Infrastructure Protection and Information Assurance (Objectives 1 and 7 above)

- CIO-SP2i Task Area 9. Software Development (Objectives 1, 5 and 8 (post Full Operational Capability) above)

5. Specific Tasks

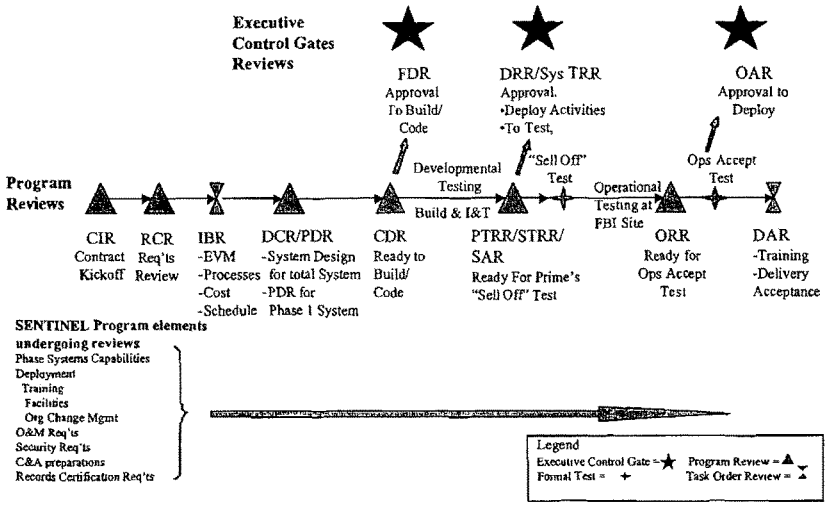
The Government's objective is to receive a sustainable and maintainable delivery approximately every 12 months (Operational Readiness Review from FBI IT LCMD). Each delivery shall constitute an incremental Phase. Each Phase, when deployed, represents a standalone set of capabilities that can be added to by subsequent Phases to achieve the SENTINEL Objectives. Phases may overlap each other, e.g., Phase 1 may be in system development and test while Phase 2 is in system design. SENTINEL capabilities are established in the System Requirements Specification (SRS) and CONOPS. The Incremental Development Plan contains the phase content description.

A delivery is considered accepted with installation and training at all operational locations and the successful completion of site acceptance testing, records management certification, the achievement of Approval to Operate (or an Interim Approval to Operate), and a successful Operational Acceptance Review (ref. FBI IT LCMD). This delivery acceptance will be the focus of a program-level review entitled Delivery Acceptance Review (DAR). The DAR shall include confirmation of all contractor work products provided to the Government for the delivery.

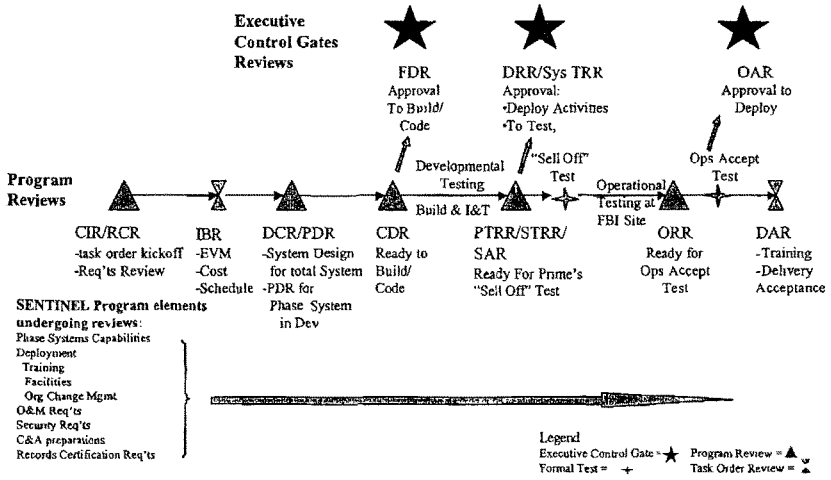
SENTINEL capabilities are established in the System Requirements Specification (SRS) and CONOPS. The Incremental Development Plan contains the Phase content descriptions.

The Phase 1 Development and Deployment and Phase 1 Organizational Change Management shall comprise the basic task order. Phases 2 – 4 Development and Deployment, all Operations and Maintenance, and Phase 2 – 4 Organizational Change Management shall be priced task order options.

The Government has applied the following tailoring to the FBI IT LCMD Control Gates and Program Reviews for Phase 1:



The Government has applied the following tailoring to FBI IT LCMD Control Gates and Program Reviews for Phases 2-4:



The SENTINEL Prime Contractor shall conduct the Program Reviews. The SENTINEL Government Program Management Office will conduct the Control Gate Reviews using an executive summary of the material provided by the contractor at the Program Reviews.

Additionally, in accordance with the FBI IT LCMD process, as Phases 2-4 constitute priced task order options; the Government Program Management Office will obtain separate Acquisition Plan Review, FBI

IT LCMD Control Gate 2, approvals prior to task order option awards for CLINs 2, 3, and 4 (notional, section 9.2)

5.1 Task 1-Contract-Level and Task Order (TO) Management

5.1.1 Task 1 Subtask 1-Contract-Level Program Management

The contractor shall provide the technical and functional activities at the contract level needed for program management of this SOW. The contractor shall also provide the centralized administrative, clerical, documentation and other related functions.

Performance of this subtask support shall be included for all subtasks within this task order as NotSeparately Priced (NSP) Items.

5.1.2 Task 1 Subtask 2-Task Order Management

The contractor shall manage all effort resulting in the delivery of SENTINEL. The contractor's management effort shall include administration, program controls, product effectiveness, data and configuration management, risk management, subcontract management, and security management.

The contractor shall define, execute, and manage SENTINEL incremental Phases' development and deployment through the application of an Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) approach. Additionally, the IMP and IMS shall reflect the FBI IT LCMD requirements for SENTINEL Program and Control Gate Reviews. The contractor shall plan and execute against a set of processes tailored for this task order.

The contractor shall establish a Work Breakdown Structure (WBS) for SENTINEL down to at least Level 6 in order to fully describe the contractor's work effort. Consider the SENTINEL program as Level 1. Additionally, no labor driven non-level of effort work packages shall exceed 30 calendar days. The WBS numerical framework shall be applied to the IMP, IMS and cost reporting system that will establish a single common framework across the program for management, tracking and reporting. The numerical framework directly links the WBS with the IMP, IMS and cost which will provide a single SENTINEL reporting framework.

The contractor shall ensure that there is a single set of implementing processes used by all including subcontractors in carrying out the tasks and activities contained in the IMP, IMS and SOW Tasks 1, 2, 3, 4 and 5. Utilization of a single set of implementing processes shall be verified at the Contract Implementation Review.

The contractor shall: establish and execute the technical approach; organize resources; and establish and execute management controls to ensure the cost, performance and schedule requirements of the task order are met.

5.1.2.1 Earned Value Management System (EVMS) Implementation

The contractor shall establish an earned value management system immediately after contract award. The contractor shall present their earned value management system and their earned value baseline (EVMS Report) to the Government for review, comment, and the Contracting Officer's approval as part of an Integrated Baseline Review (IBR). The IBR shall occur no later than 14 calendar days after the start of the Requirements Clarification Review (RCR). The contractor's earned value management system shall comply with all of the common criteria contained in ANSI/EAS Standard 748 (current version at the time of solicitation).

The contractor shall manage and report against the established earned value management system and the established earned value baseline beginning immediately after contract award. This earned value

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00128 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.089

management and earned value reporting shall continue through the completion of the contract. The contractor shall prepare and submit a status report to the Contracting Officer at least monthly (Gregorian calendar) that details the contractor's most recent performance against the established earned value baseline. The monthly reports shall clearly distinguish between performance against the earned value baseline as a whole and performance against the portions of the earned value baseline that are not related to work packages measured using a Level of Effort (LOE) methodology.

In addition to the common criteria contained in ANSI/EAS Standard 748, the contractor's earned value management system, the contractor's earned value baseline, and the contractor's monthly earned value status reports shall comply with the detailed requirements contained in SOW Attachment-1, Earned Value Management System Requirements of this Statement of Work. In the event that there is ambiguity and/or conflict between ANSI/EAS Standard 748 and Attachment-1, the requirements of Attachment-1 shall prevail.

5.1.2.2 Risk Management Program

The contractor shall perform risk management in accordance with its corporate policy and the requirements contained in the FBI SENTINEL Risk Management Plan.

The contractor shall implement a formal risk management process that encompasses: risk management planning and budgeting; risk identification, assessment, and analysis; risk contingency planning; and risk monitoring and control (including decision procedures for escalation and exercising contingency options).

5.1.2.3 Configuration Management (CM) Program

The contractor shall perform configuration management in accordance with its corporate policy and the requirements contained in the FBI SENTINEL CM Plan and the FBI IT LCMD.

The contractor shall implement a formal CM program that includes Configuration Identification, Change Management, Configuration Status Accounting, Audit, and Release Management. The contractor shall comply with all Government CM processes and procedures as outlined in the Government's SENTINEL CM Plan. The contractor shall perform all CM activities until contract completion. The contractor shall ensure that all subcontractors and vendors comply with the CM requirements levied by the Government's CM Plan and this SOW.

5.1.2.4 Quality Assurance (QA) Program

The contractor shall perform quality assurance to include activities such as defect tracking, root cause analysis, peer reviews of all development artifacts, and appropriate levels of testing in accordance with corporate practices and the requirements of this SOW.

5.1.2.5 Security Management (facilities and personnel)

The contractor shall perform security management in accordance with the SOW Attachment-2 Contract Security Classification Specification (DD Form 254) and the additional security requirements outlined in this SOW.

5.1.3 Task 1 Subtask 3-Data Management Program

The contractor shall implement and maintain a single data management program that contains the data and information used in managing the contractor's SENTINEL program. The contractor shall provide the Government direct insight into the current program state through a data management repository. This data management repository shall be on-line and accessible from the Government program office(s) and spaces at the contractor's facility. The data repository shall include all materials generated during the program execution. Data shall include, but is not limited to, activity artifacts and results from: requirements

management and verification, architecture management, configuration management, quality assurance, risk management, earned value management, and program schedule data.

The contractor shall provide training and training materials on how the Government can achieve insight into the state of program through the data management program. The training shall cover each of the management support tools the Government shall be able to access through the data management program. For cost estimating purposes, the contractor shall assume 4 semi-annual training sessions, to be held in Government program office spaces, with the first training session consisting of 12 Government-identified personnel, and for up to 6 Government-identified personnel in each remaining session.

5.1.4 Task 1 Subtask 4-In Progress Review Support

The contractor shall provide a monthly status report containing the status of all ongoing SOW tasks. Topics to be addressed include: the Earned Value, schedule, risks, program and risk management metrics, quality assurance, configuration management, data deliveries, 6month staffing forecast, and security management applied to the task order. The contractor shall participate with the Government in formal monthly reviews and informal weekly status reviews. Contractor participants in the formal monthly reviews shall be empowered to aceept and make commitments on behalf of the contraetor, within the limits of the SENTINEL contract.

5.1.5 Task 1 Control Gates and Program Reviews

The following control gates and program reviews (ref. FBI IT LCMD) are applicable to this activity:

- Contract Implementation Review (within 14 calendar days of contract award)
- Integrated Baseline Review (within 14 calendar days of the requirements clarification review)(described in Attachment 1)
- In-Progress Review (monthly) (deseribed in SOW paragraph 5.1.4)

5.1.6 Task 1 Deliverables

A listing of data items applicable to this task is provided in SOW paragraph 9.1.

5.2 Task 2-SENTINEL Systems Engineering and Architecture

The contractor shall implement the systems engineering and architecture activities required to precede and support phase level planning, design, development, integration, test, deployment, and operations and maintenance activities.

5.2.1 Task 2 Subtask 1-SENTINEL Systems Engineering Management

The contractor shall implement a tailored systems engineering approach for defining, designing, developing, integrating, testing, and deploying SENTINEL's capabilities in incremental Phases. This approach shall be based upon the contractor's established Systems Engineering Methodology and implementing processes. The contractor shall include architecture development, system development, integration and test, and deployment as part of its systems engineering approach. This approach shall be described in its Systems Engineering Management Plan and be visible in the Integrated Master Plan, Integrated Master Schedule, and reflected in the Work Breakdown Structure.

The contractor shall support the FBI IT LCMD control gates and project reviews for the SENTINEL program and its incremental Phases implementation.

The contractor shall develop and utilize a specification hierarchy in determining and producing a necessary set of technical documents that describes the SENTINEL technical baseline. This technical baseline shall be updated upon commencing of a Phase's deployment to the FBI Enterprise. The contractor specification

hierarchy shall commence with a SENTINEL System Specification that validates the SRS and translates its functional and performance requirements into system specifications.

The contractor shall prepare and maintain a system specification in response to the Government SRS. The Government will retain management of the SENTINEL SRS.

The contractor shall manage all requirements and specifications for SENTINEL below the SRS level. The contractor shall allocate system requirements to capabilities. The contractor shall identify the system requirements that will be satisfied in part or completely at the end of each of Phase. The contractor shall determine the verification method of each system requirement. For those system requirements developed and delivered incrementally (i.e., in more than one Phase), the contractor shall indicate the level of system requirement capability by Phase and the method of verification in each Phase.

As noted in the SRS, Sentinel will require information sharing with systems classified higher than Collateral Secret (e.g., with Intelligence Community) and with systems at a lower classification level (e.g., state and local law enforcement). This will require the offeror to address Controlled Interface Guards (see, e.g., http://www.dtic.mil/whs/directives/corres/html2/d46305x.htm). The specific networks and data types to be addressed at both the high side and low side are to be determined, but the offeror will have to address this capability in the proposed system design.

For all system performance requirements (e.g., availability, throughput, responsiveness of the system), the contractor shall develop, document, and maintain planned technical performance profiles, and associated out-of-band reporting profiles, that span the entire SENTINEL development. As actual data becomes available, the contractor shall include the actual values in the profiles. The contractor shall identify the system performance requirements that will be satisfied in part or completely at the end of each Phase.

The contractor shall develop and utilize a system level Test and Evaluation Master Plan (TEMP) that accommodates SENTINEL evolution across its Phases and with an evolving FBI Enterprise. The Government TEMP provides a framework of specific areas that should be addressed in the contractor's SENTINEL TEMP. The contractor TEMP shall be consistent with the test approach outlined in the Government TEMP. The TEMP shall also include the contractor's integration and test facility that supports its approach, its test processes, Certification & Accreditation (C&A) approach, records management certification approach, and test data requirements.

SENTINEL has been designated a National Security System. As such, it must meet requirements set by National Information Assurance Partnership (NIAP) and National Security Telecommunications and Information Systems Security Policy (NSTISSP)-11. (General information is available at: http://niap.nist.gov/cc-scheme/nstissp-11-faqs.pdf). There are two general cases that may be applicable to the SENTINEL program and that the contractor shall account for in their design and development activities:

1. If an approved U.S. Government protection profile exists for a particular technology area, but no validated products that conform to the protection profile are available for use, the acquiring organization must require, prior to purchase, that vendors submit their products for evaluation and validation by a NIAP laboratory or Common Criteria Recognition Arrangement (CCRA) laboratory to a security target written against the approved protection profile or acquire other U.S.-recognized products that have been evaluated under the sponsorship of other signatories to the CCRA.

2. If no U.S. Government protection profile exists for a particular technology area and the acquiring organization chooses not to acquire products that have been evaluated by the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) or CCRA laboratories, then the acquiring organization must require, prior to purchase, that vendors provide a security target that describes the security attributes of their products, and that vendors submit their products for evaluation and validation at a Designated Accrediting Authority (DAA)-approved Evaluation

Assurance Levels (EAL). Robustness requirements, mission, and customer needs will together enable an experienced information systems security engineer to recommend a specific EAL for a particular product to the DAA. In addition, the organization should file the necessary for a Deferred Compliance Authorization (DCA) (see FAQ #12 under Policy Information and Guidance http://niap.nist.gov/cc-scheme/nstissp-11-faqs.pdf).

In support of the delivery of a service-based solution, the contractor shall recommend to the Government an SOA governance approach. SOA Governance addresses the technical and business aspects of using and deploying services, and provides a review process to ensure that services are managed throughout their lifecycle. This requires appropriate definition of the procedures and policies to be complied with when making a service available to SENTINEL and/or to the Enterprise, and when any change is proposed to an approved service. The proposed Governance approach should address who is allowed to publish a service to the registry, establish the release procedures, and determine the approval and certification process for designs, standards and security policies. It should propose how to perform governance validation before allowing services to be published and how the FBI should follow that up by continued policy checks during use. The contractor shall participate in the governance process, once approved, as required by the process in the deployment of SENTINEL.

The contractor shall support the Government certification and accreditation process defined in the FBI Certification and Accreditation Handbook. This includes preparation for and support of Certification and Penetration Test and Evaluation as well as support to recurring Security Test and Evaluation once the system is operational.

The contractor shall support the Government Records Management Certification process defined in the FBI Electronic Recordkeeping Certification Manual.

The contractor shall support Government Independent Verification and Validation (IV&V) activities. The IV&V activities include monitoring the design, development and test, implementation and integration of SENTINEL. The Government IV&V activities are scoped as monitoring and oversight.

5.2.2 Task 2 Subtask 2-SENTINEL Architecture Management

The contractor shall develop, document, and maintain a SENTINEL architecture that (1) permits the incremental implementation and deployment of functional capabilities, (2) is scalable, flexible, and modular, and (3) leads to an easy to use system that users can access through the FBINet. The contractor shall conduct trade studies as required to define the architecture and to determine hardware and software.

The contractor shall develop a SENTINEL Target Architecture, with phased increments, that achieves SRS capabilities in deployable standalone Phases that can be added to by subsequent Phases to expand capabilities. Each Phase shall have its own architecture representation establishing the set of SENTINEL SRS capabilities that will be delivered.

The SENTINEL Target Architecture shall be compatible with and address the intent depicted in the FBI EA Target Architecture Report to the maximum extent possible. The contractor shall develop an architecture that conforms to the Government TRM to the extent practical. The contractor shall identify planned deviations from the TRM to the Government.

The contractor shall develop, model, document, and maintain materials sufficient to describe the architecture and business-driven performance criteria throughout the life of the system to include the development of business scenarios to validate the integrity of architecture. Performance analyses shall include the impact of implementing SENTINEL on FBINet.

5.2.3 Task 2 Control Gates and Program Reviews

The following control gates and program reviews (ref. FBI IT LCMD) are applicable to this activity:

- Requirements Clarification Review (2 weeks after CIR for Phase 1, in conjunction with CIR for Phases 2-4)
- Design Concept Review (in conjunction with Phase PDR)

5.2.4 Task 2 Deliverables

A listing of data items applicable to this task is provided in SOW paragraph 9.1.

5.3 Task 3-Phase Design, Development, Test, Implementation, and Integration

The contractor shall conduct all activities necessary to design, develop, integrate, test and deploy an incremental Phase that provides a set of defined capabilities and implements and integrates them with the existing FBI infrastructure.

The contractor shall create and maintain plans for Phase transition, deployment, and installation.

The contractor shall support the Government Certification and Accreditation process defined in the FBI Certification and Accreditation Handbook.

The contractor shall support the Government Records Management Certification process defined in the FBI Electronic Recordkeeping Certification Manual.

The contractor shall support Government Independent Verification and Validation (IV&V) activities. The activities include monitoring the design, development and test, implementation and integration of SENTINEL. The Government IV&V activities are scoped as monitoring and oversight; no independent testing of the system is planned as part of IV&V.

Support to Government testing includes: providing access to a correctly configured and documented system, keeping the system operational, providing access to all requested documentation; operating the system; performing the procedures during security testing and certification testing, and answering questions including showing system and software configuration details. The contractor shall also be required to establish (and remove at the completion of testing) test accounts (both general and privileged) as required in the test plan and procedures.

5.3.1 Task 3 Subtask 1-Phase Design

The contractor shall perform IMP and IMS engineering activities to ensure that each Phase satisfies the requirements allocated to it. The contractor shall decompose Phase requirements to the lowest level to effectively and efficiently complete the Phase detail design activities. The contractor shall create and maintain a verification matrix of the Phase's system level requirements.

The contractor shall develop, document, and maintain all internal interface requirements including the Document Creation Ingest Specification identified in the SRS.

The contractor shall develop, document, and maintain the SENTINEL side of all external interface requirements in conjunction with the parties responsible for other systems.

The contractor shall provide justification for the use of selected COTS products and any proposed custom development.

The contractor shall conduct all design activities necessary to create, maintain, and deploy each Phase (includes the underlying data) such that each Phase meets all system requirements, security and records management accreditation requirements and attains an Approval to Operate.

5.3.2 Task 3 Subtask 2 Phase Development and Test

The contractor shall acquire or develop all hardware and software components required to implement the approved Phase design. The contractor shall assemble, configure, integrate, and test all software and hardware components that are part of the Phase design in preparation for system level testing.

The contractor shall create and maintain Phase test plans, procedures, and test cases at all levels as outlined in the contractor TEMP. The contractor shall create and maintain a traceability of Phase requirements, including related interface requirements, to test cases. The contractor shall document the results of all testing.

The contractor shall test the readability and formatting of all migrated data in preparation for system level testing.

5.3.3 Task 3 Subtask 3-Phase Implementation and Integration

The contractor shall perform all activities necessary to execute system level functional, performance, interface, and integration testing of each Phase in factory, limited-deployment, and full-deployment (operational) environments.

The contractor shall perform all activities necessary to deploy each Phase, including the supporting hardware, software, and data, to the operational locations. These activities include, but are not limited to, packaging, shipping, delivery, installation, integration, configuration, and check-out.

The contractor shall perform all activities necessary to fully configure all capabilities for operations. This includes delivering and installing all the software, initializing configuration files, configuring all of the accounts, establishing the organizational infrastructure to support workflow, defining all communities of interest and roles to support access controls. For the records management application, the contractor will implement the FBI provided file plan with the selected COTS software product. For the migrated data, the vendor will populate the record folder components and the record components with the appropriate metadata. The RM metadata will assist Records Management Division (RMD) in the management of FBI records.

The contractor shall perform all activities (extract, translate and error correction, load) necessary to migrate legacy data needed for the operation of capabilities delivered in each Phase. The contractor shall verify that no data required was lost or corrupted during the migration process. The contractor shall perform error correction as part of the data migration task. In support of legacy system shutdown, the contractor shall perform all activities necessary to migrate all necessary legacy data.

The contractor shall support the acceptance and transition of each Phase to full operations. The contractor shall support user acceptance test activities at the first user implementation site. For cost estimating purposes, the contractor shall assume a level of support of not more than two full-time equivalent staff for 60 working days (standard 8 hour work day) at a Washington Metropolitan area location.

The contractor shall support Government testing as outlined in the FBI SENTINEL TEMP. In support of Government tests, the contractor support activities shall include but not be limited to, keeping the system under test operational, providing access to all requested documentation; operating the system; performing requested procedures; answering questions and showing system and software configuration details. The contractor shall also establish and remove test accounts as required (both general and privileged).

5.3.4 Task 3 Subtask 4-Operations and Maintenance Support

In support to ongoing operations and maintenance, the contractor shall prepare and deploy modifications, patches and updates based on Government approved change requests to keep the deployed system operational. As applicable, these modifications, patches and updates shall be rolled forward into the

ongoing Phase baseline. All change requests will be approved by the Technical Configuration Control Board (TCCB) and the Change Management Board (CMB).

The contractor shall utilize implementing processes as mutually agreed to by the Government and the contractor.

The contractor shall utilize its technical governance processes for all changes recommended to the deployed technical baseline.

The contractor shall draft and forward for approval an O&M Service Level Agreement that meets the intent of the Task 4 Tiers -1 through -4 level of O&M support.

5.3.5 Task 3 Control Gates and Program Reviews

The following control gates and program reviews (ref. FBI IT LCMD) are applicable to this activity:

- Preliminary Design Review/ in conjunction with the DCR (for each Phase)
- Critical Design Review (for each Phase)
- Gate 3 - Final Design Review (FDR) (for each Phase)
- Product Test Readiness Review/Site Test Readiness Review/Site Acceptance Review (for each Phase)
- Gate 4/5 - Deployment Readiness Review/System Test Readiness Review (for each Phase)
- Operational Readiness Review (for each Phase)
- Gate 6 - Operational Acceptance Review (for each Phase)
- Delivery Acceptance Review (DAR) (for each Phase)

5.3.6 Task 3 Deliverables

A listing of data items applicable to this task is provided in SOW paragraph 9.1.

5.4 Task 4-IT Operations and Maintenance

As directed by the Government, the contractor shall perform operations and maintenance for each deployed Phase (primary, backup and training string when deployed) at the levels of performance specified in the Government approved SLA.

A ramping up period prior to the formal start of operations and maintenance shall be required. During this period the contractor shall identify and train the staff needed to operate and maintain the system in sufficient time for the staff to participate as required in the operational testing (operational test and security test and evaluation) of the system. Formal Operations and Maintenance periods begin with a successful exit from the Operational Readiness Review at each increment. The contractor must coordinate with the Transition Management Unit (TMU) in FBI's Information Technology Operations Division (ITOD) to acquire an Operational Readiness Review (ORR) at each completed Phase.

The FBI ITOD operates on a four-Tier operations support structure. Each Tier is defined below.

Tier-1 Support:

- **What:** Provides remote helpdesk support to the end user (customer) from a phone call to the Enterprise Operation Center (EOC) via 202-324-1500.

- **When:** On-site support is available 24x7x365 day a year.
- **How:** The FBI's automated call distribution software routes the call to the first available helpdesk technician for support. The technician opens a call ticket via the FBI's trouble ticketing software product (Peregrine Systems ServiceCenter™). If the helpdesk technician can resolve the issue then the call ticket is closed. If the helpdesk technician cannot resolve the issue then a problem ticket is created from the call ticket and assigned to a Tier-2, Tier-3 or Tier-4 support entity (assignment group) for resolution. The ticket automatically is displayed in the assignment group's problem queue.
- **Functions:** Taking the customers call, creating call ticket, generating problem ticket (if necessary), remote troubleshooting, answering questions, password administration (resets, unlocks, unsuspend), profile related issues, desktop software and OS related issues, resolving user specific issues (not network, server, system, application or database issues), checking Tier-1 problem queue for tickets and reassigning (routing) them to the appropriate Tier-2, Tier-3 or Tier-4 assignment groups.

Tier-2 Support:

- **What:** Provides touch labor (on-site) support to systems and desktops, remote server and network support, remote account administration.
- **When:** On-site support is available during normal business hours, on-call evenings and weekends. The EOC (SysAdmin/Network) is available on-site 24x7x365 days a year.
- **How:** Tier-2 support groups are responsible for checking their problem queues, acknowledging, assigning and updating ticket with status of troubleshooting. Once the issues are resolved, the Tier-2 Group is responsible for ensuring the integrity of the ticket, entering appropriate resolution, contacting the customer (when appropriate) and closing the ticket. When appropriate, the Tier-2 Group is responsible for preparing scripts or procedures to document corrective actions for lower tier support use.
- **Functions:** Monitoring of enterprise networks and system enclaves, monitoring of enterprise and system servers, remote network and server support, remote server and desktop virus updates, desktop hardware support, laptop support, network hardware support, account administration (new, modified or deleted account).

Tier-3 Support:

- **What:** Provides application, systems, network, server and mainframe support.
- **When:** On-site support is available during normal business hours, on-call evenings and weekends.
- **How:** Tier-3 support groups are responsible for checking their problem queues, acknowledging, assigning and updating ticket with status of troubleshooting. Once the issues are resolved, the Tier-3 Group is responsible for ensuring the integrity of the ticket, entering appropriate resolution, contacting the customer (when appropriate) and closing the ticket. When appropriate, the Tier-3 Group is responsible for preparing scripts or procedures to document corrective actions for lower tier support use.
- **Functions:** OS patch management

Tier-4 Support:

- **What:** Provides support to systems ' databases, re-engineering or issues that occur outside of normal operations.
- **When:** On-site support is available during normal business hours, on-call evenings and weekends.
- **How:** Tier-4 support groups are responsible for checking their problem queues, acknowledging, assigning and updating ticket with status of troubleshooting. Once the issues are resolved, the Tier-4 Group is responsible for ensuring the integrity of the ticket, entering appropriate resolution, contacting the customer (when appropriate) and closing the ticket. When appropriate, the Tier-4 Group is responsible for preparing scripts or procedures to document corrective actions for lower tier support use.

- **Functions**: Re-engineering of current system, software licensing & maintenance support, resolving database errors or enhancements to current databases, testing enhancements to applications and baselines.

The contractor shall implement an operations and maintenance approach consistent with the Tier approach as defined above. The FBI's ITOD will perform Tier-1 activities. Coordinating jointly with the FBI's ITOD, the contractor shall be responsible for Tiers-2, -3 and -4 activities.

Definition of Normal Business Hours: 7:30 a.m. – 4:00 p.m. EST (Monday – Friday).

5.4.1 Task 4 Subtask 1-Pre-Full Operational Capability (FOC) Operations and Maintenance (separately priced options for O&M of each Phase)

Note: FOC occurs at the completion of the final incremental Phase (Phase 4) deployment

5.4.1.1 Conduct System Administrator Training

The contractor shall conduct training in accordance with the approved Training Plan. The contractor shall provide training for SENTINEL Phases prior to them being delivered. The contractor shall be responsible for the generation and distribution of all training materials.

5.4.1.2 Conduct of Pre-FOC Operations and Maintenance

Note that Tier-4 activities are addressed under Task 3 during Pre-FOC Operations and Maintenance.

The contractor shall conduct Tier-2 and Tier-3 operations and maintenance as required for each deployed Phase to ensure the service levels agreed to in the SLA are sustained and the system certification is maintained. Operations tasks include, but are not limited to:

- System administration including performance of authorized configuration changes (e.g., adding user accounts, changing passwords, modifying workflow groups) in accordance with the established procedures.
- Develop and maintain scripts and procedures in support of Tier-1, -2, -3, and -4 activities.
- Maintain an inventory of hardware and software on site and perform site configuration management. Equipment that is purchased for SENTINEL must be placed in the FBI's Property Management Application (PMA). Inventory of Hardware and Software shall be managed by the contractor.
- Maintain system security in accordance with the approved procedures. The hardware being proposed for SENTINEL must be capable of supporting the FBI's existing security policies.
- Make software changes/corrections as directed by the Government and in accordance with FBI CM procedures.
- Ensure all documentation is updated as changes are made in accordance with CM procedures.
- Interact closely with ITOD for purposes of knowledge transfer, roll changes into next release, etc.
- Conduct Hardware and Software License and Warranty Management including coordinating with FBI ITOD for warranty support for items covered under the FBI's enterprise warranties.
- Deploy and test patches, updates, and other modifications in accordance with approved Patch Management procedures (SUS Patch Management Roadmap and associated procedures).
- The contactor shall maintain the established configuration baseline and adhere to the established configuration management process.
- The contractor will need to provide CM resources for the following CM activities: Configuration Identification, Change Management, Configuration Status, Accounting, Audit, and Release

Management. These CM Activities are defined in the FBI CM Plan.

- Maintain the offline environments (e.g. development, test, staging, etc.) required to support operations and maintenance activities.
- Respond to and resolve problem tickets in the amount of time agreed to in the SLA.

Any actions or changes not explicitly authorized via the baselined O&M and accreditation documents shall be documented via a Change Request. The Government will approve all Change Requests. All proposed baseline changes shall be reviewed for impact to both the operational and development baseline. The Government will be the approving authority for all Change Requests utilizing the process defined in the FBI CM Plan.

5.4.2 Task 4 Snbtask 2-Operations and Maintenance Transition (separately priced option)

The Government may choose to transition Operations and Maintenance immediately following the FOC deployment or at any time during the two years following the FOC deployment. In the event that not all Phase options are exercised, the Government may initiate the transition task in conjunction with or following the last exercised Phase option.

5.4.2.1 Condnct System Administrator Training

The contractor shall conduct training in accordance with the approved Training Plan. The contractor shall provide training for SENTINEL Phases prior to them being delivered. The contractor shall be responsible for the generation and distribution of all training materials.

5.4.2.2 Condnct Operations and Maintcnance

Upon request, the contractor shall implement and ensure a seamless transition of Tiers -2, -3 and -4 operations and maintenance activities to the FBI ITOD within a 6-month period. The transition task shall include but is not limited to:

- Classroom and on the job training of system administrators and privileged users.
- Collaborative conduct of operations and maintenance during the transition period.
- Identify number of resources and skill set required by the FBI to assume O&M responsibilities.
- Develop Roles and Responsibilities for the different ITOD entities for O&M functions.
- The contractor shall hold briefings to educate the FBI about trace O&M entitlement, subcontracting accomplishments, and all related requirements that were developed on behalf of the FBI.
- Transition all hardware, software, and licenses to the FBI (ITOD). All warranty and maintenance terms need to be documented and provided to the FBI.
- Ensure that all System documentation is current.
- Development of an O&M transition plan as defined in the list of Deliverables.

During the designated transition period, the contractor shall be responsible for the established SLAs.

5.4.3 Task 4 Subtask 3 Post-FOC Operations and Maintenance and Sustainment (separately priced options for two one-year periods)

5.4.3.1 Conduct System Administrator Training

The contractor shall conduct training in accordance with the approved Training Plan. The contractor shall provide training for SENTINEL Phases prior to them being delivered. The contractor shall be responsible for the generation and distribution of all training materials.

5.4.3.2 Conduct Operations and Maintenance

The contractor shall conduct operations and maintenance (Tier-2, -3, and -4) for the FOC system ensuring the service levels agreed to in the SLA are maintained and the system certification is maintained. Tasks include, but are not limited to:

- Planning for and implementation of a technology refreshment program.
- System administration including performance of authorized configuration changes (e.g., adding user accounts, changing passwords, modifying workflow groups) in accordance with the established procedures.
- Develop and maintain scripts and procedures in support of Tier-1, -2, -3, and -4 activities.
- Maintain an inventory of hardware and software on site and perform site configuration management. Equipment that is purchased for SENTINEL must be placed in the FBI's Property Management Application (PMA). Hardware and software inventory shall be managed by the contractor.
- Maintain system security in accordance with the approved procedures.
- Make software changes/corrections as directed by the Government and in accordance with FBI CM procedures. Note that post FOC, all Tier 4 activities are conducted under Task 4.
- Ensure all documentation is updated as changes are made in accordance with CM procedures.
- Conduct Hardware and Software License and Warranty Management.
- Deploy and test patches, updates, and other modifications in accordance with approved Patch Management procedures. Refer to Section 15 for details.
- The contactor shall maintain the established configuration baseline and adhere to the established configuration management process.
- The contractor will need to provide CM resources for the following CM activities: Configuration Identification, Change Management, Configuration Status, Accounting, Audit, and Release Management. These activities are defined in the FBI SENTINEL CM Plan
- Respond to and resolve problem tickets in the amount of time agreed to in the SLA.

Any actions or changes not explicitly authorized via the baselined O&M and accreditation documents shall be documented via a Change Request. The Government will approve all Change Requests. All proposed baseline changes shall be reviewed for impact to the operational baseline. The Government will be the approving authority for all Change Requests utilizing pre-defined boards.

5.4.4 Task 4 Control Gates and Program Reviews

The following control gates and project reviews (ref. FBI IT LCMD) are applicable to this activity:

- Annual Operations Review

5.4.5 Task 4 Deliverables

A listing of data items applicable to this task is provided in SOW paragraph 9.1.

5.5 Task 5-Organizational Change Management

As SENTINEL services are deployed, the FBI will dramatically change its way of doing business. To ensure a smooth transition and full adoption by the SENTINEL customer base, an organizational change management program is needed.

The contractor shall perform all activities necessary to develop and implement an effective Organizational Change Management program. The contractor shall market, develop training materials, conduct training and provide continued user support as required to ensure full adoption of SENTINEL and its associated business processes. All user contact shall be conducted in coordination with the Government program office.

5.5.1 Task 5 Subtask 1-Assess and Plan Change Management

The contractor shall work collaboratively with FBI personnel to analyze and develop the SENTINEL Stakeholder and Organizational Risk Assessment (SSORA). This information shall be a critical input to Workforce Transformation (WFT) activities during subsequent SENTINEL deployments. This document shall provide input to workforce transition plans and activities required for successful transition to new roles and responsibilities of end users, the communication and stakeholder management plan, and the development of a training plan.

The SSORA will serve as a guide for detailed planning and execution of all SENTINEL change management activities.

The contractor shall analyze and generate an Organization Impact Assessment (OIA) to identify organization-wide impacts of SENTINEL on FBI law enforcement processes and/or systems. The contractor shall follow the SENTINEL Risk Management process to document any risks identified in the OIA.

The contractor shall develop a Workforce Transformation Strategy and Plan based on the SSORA and OIA.

5.5.2 Task 5 Subtask 2-Develop Training Material

5.5.2.1 Training Strategy and Plan

The contractor shall develop and implement a detailed SENTINEL Training Strategy and Plan for FBI users that relates SENTINEL processes by Phases to deployment schedules. The plan shall identify how to leverage and seamlessly integrate Technology Based Training (TBT) (e.g., Web-based, computer based training, distance learning) and instructor lead training across each SENTINEL Phase while managing effects on FBI law enforcement operations; identify SENTINEL user group profiles by geographic location; analyze SENTINEL training for impacts on the FBI workforce, and analyze training to accommodate steep learning curves and changes in work roles and responsibilities. The plan shall coordinate training activities with FBI wide training initiatives. The plan shall include a knowledge transfer and integration strategy for the transference of SENTINEL training to the FBI Training Academy and Field Office training teams.

The contractor shall propose a suitable user training package to accommodate both new and existing employees. Such a package may include TBTs, a user's manual and/or any other such materials identified in the approved Training Strategy and Plan.

The contractor shall analyze and report on the FBI's existing training administration processes to determine how training participation is recorded. If necessary, the contractor shall recommend a reproducible SENTINEL training administration solution, and implement the FBI approved solution for recording and tracking participation in SENTINEL training.

5.5.2.2 Training Media

Training media may include TBT, instructor-lead, user manuals (automated and written), Frequently Asked Questions (FAQs), in addition to the "context-sensitive" help embedded in the application. TBT shall be delivered from a SENTINEL website that is seamlessly integrated into the SENTINEL application. In cases where instructor-lead training is beneficial, the contractor shall arrange for an appropriately equipped facility (if the Government is unable to provide same) and trainers. Training instructors shall be certified (e.g., Amercian Society for Training and Development, FBI Academy)

5.5.2.3 Technology-Based Training

The contractor shall exploit modern TBT wherever possible and shall deliver these packages in a manner and form compatible with the SENTINEL system. The contractor shall follow the Sharable Content Object Reference Model (SCORM) which aims to foster creation of reusable learning content as "instructional objects" within a common technical framework for computer and technology-based learning. The contractor shall arrange for an appropriately equipped facility (if the Government is unable to provide the same).

5.5.3 Task 5 Subtask 3-Conduct User Training

The contractor shall conduct training in accordance with the FBI approved Training Strategy and Plan. The contractor shall provide training for SENTINEL services as they are delivered. Training will begin upon receipt of Authority to Operate; however, for the first implementation site (see paragraph 5.3.3) training must be completed immediately before the receipt of Approval to Operate. The contractor shall be responsible for the generation and distribution of all training materials.

Training shall be accomplished in a decentralized fashion at each of the FBI Field Offices and foreign Legal Attaché posts. Training shall also be accomplished at Resident Agencies with 50(FBI- *Offeror to update as appropriate based on proposed training approach*) or more field agents attached to the location.

The contractor shall develop and perform a repeatable process for analyzing and resolving user identified training problems, feedback, and lessons learned and communicate the results to the FBI Communications and performance engineering teams. The results will include a matrix categorizing the training problems. The matrix shall include the severity, frequency, and resolution plans for the problem, identifying how the curriculum will be rectified.

5.5.4 Task 5 Subtask 5-Continued User Support

The contractor shall provide user assistance (facilitators) at the selected training locations (see paragraph 5.3.3) for two weeks (target, location dependent) following the training. Travel to smaller offices may be required.

5.5.5 Task 5 Subtask 6-Extended Support

The contractor shall provide the following extended support to the new process activities: incorporation of paper-only documents, incorporation of photos, individual tutoring of field personnel, and incorporation of historical information related to open cases that have migrated to SENTINEL. For estimating purposes assume this support begins with the completion of Task 5 Subtask 5 and continues for an additional 2 weeks at each location where training is provided. Travel to smaller offices may be required.

5.5.6 Task 5 Subtask 7-Support to Government Communications

The contractor shall develop and execute a Communications Plan (CP) for audiences having interest in SENTINEL in order to promote their understanding of the benefits of SENTINEL. The CP shall describe messages tailored to each audience's perspectives and shall state how these messages will be delivered in a

timely manner through channels and in formats most relevant to each audience. Audiences of interest include: FBI employees who are not expected to be users of SENTINEL; oversight agencies and Congress; government agencies not expected to participate; the media; and groups interested in the technical and program management aspects of SENTINEL.

The contractor shall create comprehensive messages and supporting documentation, which clearly explain the mission, vision, and goals of the SENTINEL program. The contractor shall support communications activities that create awareness and understanding of the SENTINEL initiative, approaches, values, and general deployment timeframes. The contractor shall produce communications content and products that address the unique needs and roles of various audiences. The contractor shall craft communications messages containing baseline SENTINEL program information including, but not limited to, schedule, milestones, functionality descriptions, and benefits. The contractor shall conduct analyses and assessments of communications activities based on research, feedback, and lessons learned. The contractor shall use this information to develop ways to improve its communications planning, activities, and performance.

The contractor shall develop content for FBI communications products including briefings, interview talking points, presentations, internal FBI newsletters, FBI Management Toolkits, frequently asked questions (FAQs) requests, fact sheets, FBI Web portal content, Congressional questions for the record (QFRs), reports to Congress, and other media, as requested.

The contractor shall develop specific demonstrations as a communications tool (not a training tool) with accompanying User Guide of the features of SENTINEL. The demonstrations may be developed for both internal (FBI) and external stakeholders for each Phase.

5.5.7 Task 5 Control Gates and Program Reviews

The following control gates and project reviews (ref. FBI IT LCMD) are applicable to this activity:

- Requirements Clarification Review (2 weeks after CIR for Phase 1, in conjunction with CIR for Phases 2-4)
- Design Concept Review (in conjunction with Phase PDR)
- Preliminary Design Review/ in conjunction with the Design Concept Review (for each Phase)
- Critical Design Review (for each Phase)
- Gate 3 - Final Design Review (FDR) (for each Phase)
- Product Test Readiness Review/Site Test Readiness Review/Site Acceptance Review (for each Phase)
- Gate 4/5 - Deployment Readiness Review/System Test Readiness Review (for each Phase)
- Operational Readiness Review (for each Phase)
- Gate 6 - Operational Acceptance Review (for each Phase)
- Annual Operational Review (yearly after first delivery)
- Delivery Acceptance Review (DAR) (for each Phase)

5.5.8 Task 5 Deliverables

A listing of data items applicable to this task is provided in SOW paragraph 9.1.

6. Contract Type

Development and Organizational Change Management (Contract Line Item Numbers) CLINs will be awarded on a cost plus award fee basis using the performance-based SOW requirements as the basis for performance.

Material CLINs will be awarded on a cost reimbursement with fixed material handling fee. The Government reserves the right to substitute GFE for all proposed items in the material CLIN.

Travel CLINs will be awarded on a cost reimbursement basis.

Operations and Maintenance CLINs will be awarded on a cost plus award fee basis using Service Level Agreements when applicable.

7. Place of Performance

Although some work will be accomplished at FBI facilities, the primary site for work associated with this Task Order shall be the contractor's facility. Program management, systems engineering, design, development, integration and initial system level testing will be performed at the contractor's facility. Elements of implementation and integration including final system and enterprise integration testing, organizational change management, and operations and maintenance will be performed at Government facilities. The Clarksburg, WV. Data Center will serve as the primary site and the Washington D.C. Data Center as the backup and site test location. Other locations will be made available as required and requested.

8. Period of Performance

The base period of performance for Phase 1 development is nominally 12 months. Successful completion of Phase 1 is at Delivery Acceptance Review. SENTINEL's subsequent option periods are to follow a similar period of performance. Period of performance is [redacted]. *[To be proposed as part of proposal.]* The Government will provide a 30-day notice of intent before each option is to be exercised.

9. Deliverables/Delivery Schedule

9.1 Data Requirements

Table 9.1-1 contains a listing of data requirements by SOW Task. The complete delivery schedule tied to FBI IT LCMD Program Reviews is contained in Attachment-3. The Attachment 3 delivery schedule deviates from the suggested schedule contained in the FBI IT LCMD to accommodate the tailoring of the Control Gates and Program Reviews. Documents required for a given review or control gate shall be delivered as soon they are available and must be delivered no later than one week prior to the review or control gate. Delivery requirements for non-gate/review items are in Table 9.1-1 below and in the Section 18 descriptions.

Descriptions of data items can be found in the FBI IT LCMD Appendix H, the FBI C&A Handbook, and in Section 18 of the SOW. Where there are descriptions provided in both the FBI IT LCMD and in the SOW, the description in the SOW shall prevail.

The referenced Data Item Descriptions are for functional guidance as to the technical content.

Distribution of the required data is limited to authorized United States Government Agencies only.

Any contractor-imposed distribution restrictions shall be noted on the cover page, all applicable pages, and

all specific paragraphs that contain information with contractor-imposed restricted distribution requirements.

Copies of the Data Items shall be delivered in both hard copy and electronic format. Electronic format shall be in one of the following formats as applicable to the type of data delivered: Microsoft Word 2000, Microsoft PowerPoint 2000, Microsoft Excel 2000, or specific format approved by the Contracting Officer's Technical Representative (COTR).

Electronic formatted data items shall be delivered on CD-ROM disks and labeled with the document title, document number assigned by the COTR (if any), version/revision number (if any), security classification, **file type, "Preliminary," "Draft," "Final," or "Baseline" annotation, Data Item number, document date, copy information, and special handling instructions (if any). Electronic formatted data shall be virus scanned and free from any known virus in compliance with FBI security requirements.**

All data items shall be delivered electronically on CD-ROM disks to the Program Manager (PM) and in hardcopy to the PM, Contracting Officer's Technical Representative (COTR), and the Contracting Officer (CO).

Unless otherwise noted, the comment and update period is three weeks for each document: two weeks for Government review and one week for the contractor to complete the update.

All data items require Government approval unless otherwise noted.

Procedures included or referenced in the data items shall be written at the keystroke level. This guidance applies to data items including, but not limited to, the Privileged User Security Guide, General User Security Guide, System Operations and Maintenance Manual, Users Manual, and the Software Installation Manual.

Commercial hardware and software manuals shall be delivered and are suitable substitutes for the technical manual deliverables. Technical manuals are only required in the event a commercial manual is not available, off-the-shelf hardware or software is modified, or custom hardware or software is developed. Commercial manuals in conjunction with addenda are also acceptable when appropriate.

Table 9.1-1 Task Order Data Requirements

Data Item Number	Document Title	Applicable Task	Description Source
0076	Agendas, Briefings, Meeting Minutes (as required)	5.0 (all)	SOW Section 18
0073	Analysis/Trade Study Report (as required)	5.0 (all)	FBI IT LCMD App H
0015	Bill of Materials	5.1.2	FBI IT LCMD App H
0016	Configuration Management Plan	5.1.2	FBI IT LCMD App H
0004	Contract Funds Status Report (CFSR) (monthly)	5.1.2	SOW Section 18
0007	Defect Reports (monthly with Measurement Report)	5.1.2	SOW Section 18
0005	Earned Value Mgmt. Sys. (EVMS) Report (Monthly)	5.1.2	SOW Section 18
0012	EOC Memorandum of Understanding	5.1.2	SOW Section 18
0078	Integrated Master Plan	5.1.2	SOW Section 18
0014	Integrated Master Schedule (weekly)	5.1.2	SOW Section 18
0008	Measurement Plan (incl CPMs)	5.1.2	SOW Section 18
0009	Measurement Report (monthly)	5.1.2	SOW Section 18
0017	Quality Assurance Plan	5.1.2	FBI IT LCMD App H

0013	Risk Assessment (delivered twice monthly)	5.1.2	SOW Section 18
0006	Risk Management Plan	5.1.2	SOW Section 18
0003	Security Plan	5.1.2	FBI IT LCMD App H
0001	Task Order Management Plan	5.1.2	SOW Section 18
0011	Travel Plan (update quarterly)	5.1.2	SOW Section 18
0050	Version Description Document	5.1.2	FBI IT LCMD App H
0018	Data Accession List	5.1.3	SOW Section 18
0002	In Progress Review Report (monthly)	5.1.4	SOW Section 18
0034	Certification Test Plan	5.2.1	FBI C&A Handbook
0039	Data Migration Plan	5.2.1	SOW Section 18
0022	Operations and Maintenance Design Document	5.2.1	FBI IT LCMD App H
0026	Requirements Clarification Document	5.2.1	FBI IT LCMD App H
0074	Requirements Traceability Matrix	5.2.1	FBI IT LCMD App H
0030	Security Implementation Plan	5.2.1	FBI C&A Handbook
0023	System Design Document	5.2.1	FBI IT LCMD App H
0020	System Specification	5.2.1	FBI IT LCMD App H
0024	Systems Engineering Management Plan	5.2.1	FBI IT LCMD App H
0037	Test and Evaluation Master Plan	5.2.1	FBI IT LCMD App H
0047	Training Plan	5.2.1	FBI IT LCMD App H
0021	Transition Plan	5.2.1	FBI IT LCMD App H
0025	Design Concept Description and Architecture	5.2.2	SOW Section 18
0066	Logical Data Model	5.2.2	SOW Section 18
0058	Software Development Plan	5.3.0	FBI IT LCMD App H
0081	Delivery Acceptance Report	5.3.0, 5.5	SOW Section 18
0059	Database Design Document (DBDD)	5.3.1	FBI IT LCMD App H
0044	Interface Control Document	5.3.1	FBI IT LCMD App H
0045	Interface Design Document	5.3.1	FBI IT LCMD App H
0054	Systems Operations and Maintenance Manual	5.3.1	FBI IT LCMD App H
0053	Technical Manual (Non-Commercial HW only)	5.3.1	SOW Section 18
0031	General User Security Guide	5.3.2	FBI C&A Handbook
0032	Privileged User Security Guide	5.3.2	FBI C&A Handbook
0051	Software Installation Manual	5.3.2	FBI IT LCMD App H
0049	Software Product Specification	5.3.2	FBI IT LCMD App H
0028	System Security Plan	5.3.2	FBI C&A Handbook
0048	Test Procedures	5.3.2, 5.3.3	FBI IT LCMD App H
0052	Test Report	5.3.2, 5.3.3	FBI IT LCMD App H
0055	Training Materials	5.3.2, 5.5.2	FBI IT LCMD App H
0029	Certification Test Plan (ST&E) (Development)	5.3.3	FBI C&A Handbook
0041	DCU04 Request for Data Center Access	5.3.3	SOW Section 18
0042	DCU05 Request for Data Center Equipment Installation	5.3.3	SOW Section 18
0061	Installation Drawings	5.3.3	FBI IT LCMD App H

0046	Installation Plan	5.3.3	FBI IT LCMD App H
0065	Product (CSCI's)	5.3.3	SOW Section 18
0027	Contingency Plan	5.3.3	FBI C&A Handbook
0040	EOC Operational Support Requirements Document of New Systems	5.3.4	SOW Section 18
0036	Service Level Agreement	5.3.4	SOW Section 18
0068	O&M Procedures	5.3.4, 5.4	SOW Section 18
0057	Operational Readiness Report	5.3.5	FBI IT LCMD App H
0069	O&M Transition Plan	5.4.2	SOW Section 18
0071	Organization Impact Assessment	5.5.1	SOW Section 18
0070	SENTINEL Stakeholder and Organizational Risk Assessment (SSORA)	5.5.1	SOW Section 18
0077	Workforce Transformation Strategy and Plan	5.5.1	SOW Section 18
0080	Training Administration Report	5.5.2	SOW Section 18
0079	Training Strategy and Plan	5.5.2	SOW Section 18
0072	User Manual	5.5.2	FBI IT LCMD App H
0010	Communications Plan	5.5.6	SOW Section 18

9.2 Task Order Delivery Schedule (TBR)

Table 9.2-1 contains the CLIN structure and delivery schedule for the task order including the priced options.

INSTRUCTION:
As part of the proposal the contractor shall fill in the proposed durations and start and end dates in Table 9.2-1.

Table 9.2-1 Delivery Schedule

CLIN	CLIN/SUB CLIN Name	Base Contract and/or Contract Option	Applicable TORP Task Number(s)	Duration (Calendar months) TBS	Start Date (Calendar months after contract award) TBS	Finish Date (Calendar months after contract award) TBS	Contract Type	Notional Earned Value Type
1	**Phase I Development and Deployment**	**Base**	**5.1, 5.2, 5.3**				**CPAF**	**Deliverables & LOE**
1.1	Phase I Program Management	Base	5.1				CPAF	Deliverables & LOE
1.2	Phase I Systems Engineering and Architecture	Base	5.2				CPAF	Deliverables & LOE
1.3	Phase I Design, Development, Integration,	Base	5.3				CPAF	Deliverables & LOE

CLIN	CLIN/SUB CLIN Name	Base Contract and/or Contract Option	Applicable TORP Task Number(s)	Duration (Calendar months)	Start Date (Calendar months after contract award)	Finish Date (Calendar months after contract award)	Contract Type	Notional Earned Value Type
				TBS	TBS	TBS		
	Deployment, and Testing							
2	**Phase 2 Development and Deployment**	**Option**	**5.1, 5.2, 5.3**				**CPAF**	**Deliverables & LOE**
2.1	Phase 2 Program Management	Option	5.1				CPAF	Deliverables & LOE
2.2	Phase 2 Systems Engineering and Architecture	Option	5.2				CPAF	Deliverables & LOE
2.3	Phase 2 Design, Development, Integration, Deployment, and Testing	Option	5.3				CPAF	Deliverables & LOE
3	**Phase 3 Development and Deployment**	**Option**	**5.1, 5.2, 5.3**				**CPAF**	**Deliverables & LOE**
3.1	Phase 3 Program Management	Option	5.1				CPAF	Deliverables & LOE
3.2	Phase 3 Systems Engineering and Architecture	Option	5.2				CPAF	Deliverables & LOE
3.3	Phase 3 Design, Development, Integration, Deployment, and Testing	Option	5.3				CPAF	Deliverables & LOE
4	**Phase 4 Development and Deployment**	**Option**	**5.1, 5.2, 5.3**				**CPAF**	**Deliverables & LOE**
4.1	Phase 4 Program Management	Option	5.1				CPAF	Deliverables & LOE
4.2	Phase 4 Systems Engineering and Architecture	Option	5.2				CPAF	Deliverables & LOE
4.3	Phase 4 Design, Development, Integration, Deployment, and Testing	Option	5.3				CPAF	Deliverables & LOE
5	**Organizational Change Management**	**Both**	**5.1, 5.5**				**CPAF**	**Deliverables & LOE**
5.1	Phase 1 Organizational Change Management	Base	5.1, 5.5				CPAF	Deliverables & LOE
5.2	Phase 2 Organizational Change Management	Option	5.1, 5.5				CPAF	Deliverables & LOE
5.3	Phase 3 Organizational Change Management	Option	5.1, 5.5				CPAF	Deliverables & LOE
5.4	Phase 4 Organizational Change Management	Option	5.1, 5.5				CPAF	Deliverables & LOE

CLIN	CLIN/SUBCLIN Name	Base Contract and/or Contract Option	Applicable TORP Task Number(s)	Duration (Calendar months)	Start Date (Calendar months after contract award)	Finish Date (Calendar months after contract award)	Contract Type	Notional Earned Value Type
				TBS	TBS	TBS		
6	**Operations and Maintenance**	**Option**	**5.1, 5.4**				**CPAF SLA Based**	**Deliverables**
6.1	Phase 1 (pre-FOC) Operations and Maintenance	Option	5.1, 5.4				CPAF SLA Based	LOE
6.2	Phase 2 (pre-FOC) Operations and Maintenance	Option	5.1, 5.4				CPAF SLA Based	LOE
6.3	Phase 3 (pre-FOC) Operations and Maintenance	Option	5.1, 5.4				CPAF SLA Based	LOE
6.4	Year 1 Post FOC Operations and Maintenance	Option	5.1, 5.4	12			CPAF SLA Based	LOE
6.5	Year 2 Post FOC Operations and Maintenance	Option	5.1, 5.4	12			CPAF SLA Based	LOE
6.6	Operations and Maintenance Transition	Option	5.1, 5.4	6			CPAF	LOE
7	**Materials (Hardware and Software)**	**Both**	**5.1, 5.2, 5.3, 5.4, 5.5**				**CPFF**	**Deliverables**
7.1	Phase 1 Development and Deployment Materials	Base	5.1, 5.2, 5.3				CPFF	Deliverables
7.2	Phase 2 Development and Deployment Materials	Option	5.1, 5.2, 5.3				CPFF	Deliverables
7.3	Phase 3 Development and Deployment Materials	Option	5.1, 5.2, 5.3				CPFF	Deliverables
7.4	Phase 4 Development and Deployment Materials	Option	5.1, 5.2, 5.3				CPFF	Deliverables
7.5	Phase 1 (pre-FOC) Operations and Maintenance Materials	Option	5.1, 5.4				CPFF	Deliverables
7.6	Phase 2 (pre-FOC) Operations and Maintenance Materials	Option	5.1, 5.4				CPFF	Deliverables
7.7	Phase 3 (pre-FOC) Operations and Maintenance Materials	Option	5.1, 5.4				CPFF	Deliverables
7.8	Year 1 Post FOC Operations and Maintenance Materials	Option	5.1, 5.4	12			CPFF	Deliverables
7.9	Year 2 Post FOC Operations and Maintenance Materials	Option	5.1, 5.4	12			CPFF	Deliverables

CLIN	CLIN/SUB-CLIN Name	Base Contract and/or Contract Option	Applicable TORP Task Number(s)	Duration (Calendar months)	Start Date (Calendar months after contract award)	Finish Date (Calendar months after contract award)	Contract Type	Notional Earned Value Type
				TBS	TBS	TBS		
7.10	Operations and Maintenance Transition Materials	Option	5.1, 5.4	6			CPFF	Deliverables
7.11	Phase 1 Organizational Change Management Materials	Base	5.1, 5.5				CPFF	Deliverables
7.12	Phase 2 Organizational Change Management Materials	Option	5.1, 5.5				CPFF	Deliverables
7.13	Phase 3 Organizational Change Management Materials	Option	5.1, 5.5				CPFF	Deliverables
7.14	Phase 4 Organizational Change Management Materials	Option	5.1, 5.5				CPFF	Deliverables
8	**Travel**	**Both**	**5.1, 5.2, 5.3, 5.4, 5.5**				**CR**	**Deliverables**
8.1	Phase 1 Development and Deployment Travel	Base	5.1, 5.2, 5.3				CR	Deliverables
8.2	Phase 2 Development and Deployment Travel	Option	5.1, 5.2, 5.3				CR	Deliverables
8.3	Phase 3 Development and Deployment Travel	Option	5.1, 5.2, 5.3				CR	Deliverables
8.4	Phase 4 Development and Deployment Travel	Option	5.1, 5.2, 5.3				CR	Deliverables
8.5	Phase 1 (pre-FOC) Operations and Maintenance Travel	Option	5.1, 5.4				CR	Deliverables
8.6	Phase 2 (pre-FOC) Operations and Maintenance Travel	Option	5.1, 5.4				CR	Deliverables
8.7	Phase 3 (pre-FOC) Operations and Maintenance Travel	Option	5.1, 5.4				CR	Deliverables
8.8	Year 1 Post FOC Operations and Maintenance Travel	Option	5.1, 5.4	12			CR	Deliverables
8.9	Year 2 Post FOC Operations and Maintenance Travel	Option	5.1, 5.4	12			CR	Deliverables
8.10	Operations and Maintenance Transition Travel	Option	5.1, 5.4	6			CR	Deliverables
8.11	Phase 1 Organizational Change Management Travel	Base	5.1, 5.5				CR	Deliverables
8.12	Phase 2 Organizational Change Management Travel	Option	5.1, 5.5				CR	Deliverables

CLIN #	CLIN/SOW/CLIN Name	Base Contract and/or Option	Applicable TORP Task Number(s)	Duration (Calendar months)	Start Date (Calendar months after contract award)	Finish Date (Calendar months after contract award)	Contract Type	Optional Earned Value Type
				TBS	TBS	TBS		
8.13	Phase 3 Organizational Change Management Travel	Option	5.1, 5.5				CR	Deliverables
8.14	Phase 4 Organizational Change Management Travel	Option	5.1, 5.5				CR	Deliverables
9	**GWAC Fees to NIH**	**Both**	**5.1, 5.2, 5.3, 5.4, 5.5**				**GWAC FEE**	**LOE**
9.1	FY 06 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE
9.2	FY 07 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE
9.3	FY 08 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE
9.4	FY 09 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE
9.5	FY 10 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE
9.6	FY 11 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE

10. Security

10.1 Personnel and Facility Clearance Requirements

The contractor shall abide by the requirements set forth in the Contract Security Classification Specification (DD Form 254).

The contractor shall develop and maintain a comprehensive security program to address the security needs of the SENTINEL program.

The contractor shall appoint a senior official to act as the Corporate Security Officer. The individual shall interface with the FBI Security Office on all security matters, to include physical, personnel and protection of all Government information and data accessed by the contractor.

10.1.1 Personnel Requirements

Personnel clearance requirements are contained in the attached DD Form 254. Contractors who will have access to FBI facilities, systems or data shall possess an active and transferable Top Secret clearance at the time of proposal submission. The Government reserves the right to waive this requirement for any portion of the work that deals with technologies or data that is in the public domain.

10.1.2 Facility Security Requirements

Facility security requirements are contained in the attached DD Form 254.

10.2 Security Acquisition Section Requirements

10.2.1 Access to Classified Information

Notwithstanding the provisions of Section 3 of the NISPOM, the Government intends to secure services or equipment from firms that are not under foreign ownership, control or influence (FOCI) or where any FOCI, in the opinion of the Government, adversely impacts on security requirements. The Government reserves the right to contract with such Offerors under appropriate arrangements, when it determines that such contract will be in the best interest of the Government.

Accordingly, all Offerors responding to this proposal or initiating performance of a contract are required to submit a Certificate Pertaining to Foreign Interests (SF 328) or update a previously submitted SF 328, and a Key Management Personnel List (KMPL) with their proposal. All SF 328s and KMPLs shall be executed at the parent and subsidiary levels of an organization. Offerors are also required to request, collect, and forward to the Government the SF 328 from all subcontractors undertaking classified work under the Offeror's direction and control. Offerors are responsible for the thoroughness and completeness of each subcontractor's SF 328 submission. SF 328 entries should specify, where necessary, the identity, nature, degree, and impact of any FOCI on their organization or activities, or the organization or activities of a subcontractor. Additionally, a KMPL must be submitted with each SF 328 which identifies senior management by name, position, social security number, date/place of birth, and citizenship status.

The Offeror shall, in any case in which it believes that foreign influence exists or is being sought over its affairs, or the affairs of any subcontractor, promptly notify the Contracting Officer's Security Representative of all pertinent facts, even if such influence is not exerted to the degree specified in the NISPOM.

The Offeror shall provide an updated SF 328 and KMPL no later than five years from the date as certified on the last submitted SF 328. The contractor shall also promptly disclose to the Contracting Officer's Security Representative any information pertaining to any interest of a FOCI nature in the contractor or subcontractor that has developed at any time during the contractor's duration or has subsequently come to the contractor's attention. An updated SF 328 is required of the contractor or any subcontractor whenever there is a change in response to any of the 10 questions on the SF 328.

The Offeror is responsible for initiating the submission of the SF 328 and KMPL for all subcontractors undertaking classified work during the entire period of performance of the contract. Failure to comply shall be cause for default under the Default Clause of this contract.

Offerors shall complete the Certificate Pertaining to Foreign Interests (SF 328) and Key Management Personnel Listing (KMPL) for the prime contractor and all proposed subcontractors. Submission should include identification of the proposal number, name of the assigned Contracting Officer and certification of the accuracy of the provided information by an Executive Management Official of the company. Provision of false information shall be cause for default under the Default Clause of this contract.

The Government reserves the right to prohibit individuals who are not U.S. citizens from all or certain aspects of the work to be performed under this contract. The Department of Justice (DOJ)/FBI does not permit the use of non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or development of any DOJ IT system. By signing the contract or commitment document, the contractor agrees to this restriction.

Foreign Ownership, Control or Influence (FOCI) - For purposes of this clause, a U.S. company is considered under FOCI whenever a foreign interest has the power, direct or indirect, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company.

Changed conditions, such as change in ownership, indebtedness, or the foreign intelligence threat, may justify certain adjustments to the security terms under which a company is operating, or, alternatively, that a different FOCI mitigation measures be employed. If a changed condition is of sufficient significance, it might also result in a determination that a company is no longer considered to be under FOCI. **There is a continuing obligation of the selected Offeror to advise the Government of such changed conditions.** Failure to abide by this obligation shall be cause for default under the Default Clause of this contract.

Factors: The following factors will be used as the basis for making a FOCI determination. If the Offeror, or its proposed subcontractors, meet any of the following factors, they must identify themselves as a potential FOCI company and submit themselves to a Government FOCI evaluation and risk assessment:

(1) Ownership or beneficial ownership, direct or indirect, of 5 percent or more of the Offeror's company's voting securities by a foreign person.

(2) Ownership or beneficial ownership, direct or indirect, of 25 percent or more of any class of the Offeror's company's non-voting securities by a foreign person.

(3) Management positions, such as directors, officers or executive personnel of the Offeror's company held by non U.S. citizens.

(4) Foreign person power, direct or indirect, to control the election, appointment, or tenure of directors, officers or executive personnel of the Offeror's company or other decisions or activities of the Offeror's company.

(5) Contracts, agreements, understandings or arrangements between the Offeror's company and a foreign person.

(6) Loan arrangements between the Offeror's company and a foreign person if the Offeror's company's (the borrower) overall debt to equity ratio is 40:60 or greater; or financial obligations that are subject to the ability of a foreign person to demand repayment.

(7) Annual total revenues or net income in excess of 5 percent from a single foreign person or in excess of 30 percent from foreign persons in the aggregate.

(8) Ten percent or more of any class of the Offeror's voting securities held in "nominee shares", in "street names", or in some other method that does not disclose the beneficial ownership of equitable title.

(9) Interlocking directors with foreign persons and any officer or management official of the applicant company who is also employed by a foreign person;

(10) Any other factor that indicates or demonstrates a capability on the part of foreign persons to control or influence the operations or management of the Offeror's company.

(11) Ownership of 10 percent or more of any foreign interest.

Every effort must be made to ensure that supplies are provided and integrated and services are performed using sound security components, practices, and procedures. Acquisition of supplies or services from concerns under Foreign Ownership, Control or Influence (FOCI) or of supplies developed, manufactured, maintained or modified by concerns under FOCI (any or all of which shall be referred to herein as "Use of FOCI source") is of serious concern and must be approved prior to contract award and evaluated during contract performance. Approval decisions will be made on a case-by-case basis after the source or technology has been identified by the Offeror and subjected to a risk assessment.

The risk assessment process will vary depending on the acquisition type and proposed use of a FOCI source, available risk mitigation measures and the information/justification provided by the Offeror/contractor.

Any Offeror responding to this Request for Proposal (RFP), Request for Quotation (RFQ) or Sealed Bid acknowledges the Government's requirements to secure services or equipment from firms which are not under Foreign Ownership, Control or Influence (FOCI), or where any FOCI, in the opinion of the Government, adversely impacts on National Security or security requirements. The Offeror understands and agrees that the Government retains the right to reject any response to this RFP, RFQ or Sealed Bid made by the Offeror, without any further recourse by or explanation to the Offeror, if the FOCI for that Offeror is determined by the Government to be an unacceptable security risk.

Risk assessments will be on a case-by-case basis and will be used to determine whether the use of a FOCI source poses an unacceptable security risk. If an unacceptable security risk is determined, the Government retains the right to reject the use of a FOCI source or to require that certain risk mitigation measures be taken by the contractor. Similarly, the Government retains the unilateral right to approve the use of a FOCI source when the risk assessment indicates that such use would be in the Governments' best interests. If the use of a FOCI source is not approved, no classified information will be disclosed to the Offeror as part of the Government's rationale for non-approval. The Offeror (prime and subs) may not seek reimbursement from the Government for any costs associated with responding to this RFP, RFQ or Sealed Bid, as a result of a FOCI non-approval decision.

10.2.2 Products that Provide or Include Software and/or Hardware

As used in this clause, foreign-origin software and/or firmware is any software and/or firmware that is manufactured, developed, maintained and/or modified (1) outside the United States or its territories, or (2) in the United States or its territories by an individual who is not a citizen of the United States or its territories. Any degree of manufacture, development, maintenance or modification that meets either criterion (1) or (2) shall be sufficient for the software and/or firmware to be deemed foreign-origin under this clause.

The Government shall have the right to reject the offer of foreign-origin software and/or firmware during the solicitation or the supply of such software and/or firmware under the contract on a case-by-case basis. If the Government rejects the supply of foreign-origin software and/or firmware, the Government shall have the right to require a technically equal, or better, approved substitute or to terminate this contract for default. In the event that the software and/or firmware is deemed foreign-origin because of criterion (2) only, the Government shall have the right to require that the contractor not disclose the identity of the end user of the item to such individuals. In such a case, upon delivery of the software and/or firmware, the contractor shall certify that the identity of the end user was not disclosed to the individual(s).

Offeror must notify the Contracting Officer (CO) in writing at the time of submission of its proposal if any foreign-origin software and/or firmware will be included in the deliverables under the contract. When, after contract award, the contractor becomes aware of foreign-origin software and/or firmware to be delivered to the Government under the contract, the contractor shall immediately notify the CO in writing of the foreign-origin software and/or firmware to be included in the deliverables under the contract. Foreign-origin software and/or firmware that is merely a possible candidate for use under the contract shall also be identified.

Notification pursuant to this clause must include the identity of the foreign source and the nature of the software application, and is required as soon as there is a reason to know or suspect foreign-origin. Failure to provide adequate notice to the Government as specified herein can result in breach and/or default of the entire contract. If the CO does not reject foreign-origin software and/or firmware under this clause within 60 days of receiving notification, the Government's rights under this clause shall be waived.

10.2.3 Use of an Information Technology System to Support Contract Performance

Any information technology (IT) system utilized to support contract performance shall be operated in accordance with either the National Industrial Security Program Operating Manual (NISPOM) or the FBI Certification and Accreditation (C&A) Handbook.

It is a material condition of this contract that this clause be incorporated into any and all subcontracts. The certifying official as indicated on the DD Form 254 should be contacted to coordinate the required C&A process for contract performance.

Minimal requirements associated with the processing of FBI Sensitive But Unclassified (SBU), Law Enforcement Sensitive (LES), Limited Official Use (LOU), and/or For Official Use Only (FOUO) information are as follows:

1. The contractor shall designate, in writing, an individual to act as the Information System Security Officer (ISSO) responsible for this system/network.

2. The contractor is responsible for the security of all information systems used by the contractor, whether or not they connect to FBI networks, and are operated by the contractor for the FBI, regardless of location.

3. The contractor must not use or redistribute any FBI information processed, stored, or transmitted by the contractor except as specified in the contract.

4. The following constitutes the minimum set of technical security standards that must be applied to all information systems processing FBI information.

a. User Identification -- each system user shall have a unique user identification (UserId).

b. Authentication -- each system user shall be required to authenticate his UserId with a complex password.

c. Auditing -- each system shall be configured to perform auditing of system access. The following minimum information shall be captured in audit records.

(1) Identity of each user

(2) Time and date of each access

(3) Activities performed that might bypass, modify, or negate security controls

(4) Security-relevant actions associated with processing

d. Object Reuse -- each system shall clear memory and storage before reallocating space to a different user

e. Warning Banner -- a standard FBI warning banner shall be presented to each user when logging into any system processing FBI information

f. Inactivity Timeout -- an ADP system shall automatically revert to a secure condition if left inactive for a period of 15 minutes (or less) of inactivity, requiring the logged-on user to unlock the screen using a password

g. The contractor shall prepare and submit a System Security Plan (SSP) for review in support of a C&A effort.

10.2.4 Virus Control

a. The contractor certifies that it will undertake to ensure that any software to be provided or any Government Furnished Software to be returned under this contract, will be provided or returned free from any computer virus which could damage, destroy, or maliciously alter software, firmware, or hardware, or which could reveal to unauthorized persons any data or other information accessed through or processed by the software.

b. The contractor shall immediately inform the Contracting Officer when it has reasonable suspicion that any software provided or returned, to be provided or returned, or associated with the production may cause the harm described in paragraph (a) above.

c. If the contractor intends to include in the delivered software any computer code not essential to the contractual requirement, this shall be explained in full detail to the Contracting Officer.
d. The contractor acknowledges its duty to exercise reasonable care, to include the following, in the course of contract performance:

1. Using, on a regular basis, current versions of commercially available anti-virus software to guard against computer viruses when introducing maintenance, diagnostic, or other software into computers; and

2. Prohibiting the use of non-contract related software on computers, especially from unknown or unreliable sources.

10.2.5 Contracting Officer's Security Representative

Contracting Officer's Security Representatives (COSR) are the designated security representatives of the Contracting Officer and derive their authorities directly from the Contracting Officer. They are responsible for certifying the contraetor's capability for handling classified material and ensuring that customer security policies and procedures are met. The COSR is the focal point for the contractor, Contracting Officer, and Contracting Officer's Technical Representative regarding security issues. The COSR cannot initiate any course of action that may alter the terms or price/cost of the contract. The COSR for this contract is Joann Saunders and can be reached on (202) 220-9230.

11. Government Furnished Equipment (GFE)/Government Furnished Information (GFI)

11.1 Inventory Requirements

Special Provision H.15 Government Furnished Equipment, Information, or Services is applicable to this task order. Government Furnished Equipment and Information shall be returned to the Government at the completion of the task order unless otherwise directed.

11.2 Government Furnished Equipment

FBINet network and clients: SENTINEL will utilize the existing FBINet network and clients. The FBI will provide access to the FBINet and an interface to legacy systems (via the LAN at the Data Center). Available services include: WAN, LANs, Active Directory, MS Outlook, and PKI.

Enterprise monitoring system: SENTINEL is to be integrated into the existing enterprise monitoring system managed by the Enterprise Operations Center (EOC). The SENTINEL system will supply network status and alerts to the EOC utilizing standard network monitoring components (listed in SOW Section 15.5.3). The contractor will be responsible for providing personnel responsible for monitoring the SENTINEL status. The contractor shall be responsible for purchasing and installing clients/agents on SENTINEL components as needed.

Enterprise licenses: COTS software for which an enterprise or site license exists may be made available. The Government will identify any available licenses that are relevant to the contractor's SENTINEL solution during final negotiations or after award. Adjustments to the Bill of Materials will be addressed at that time.

Operational facilities: Space and infrastructure support (power, cooling, communications) in existing operational facilities will be provided for the system. Space at the Clarksburg, WV Data Center will be provided for the primary and training systems. Space at the Washington D.C. Data Center will be provided for the backup and integration test system.

Communications: The Government will provide the following Communications connectivity within 120 days, including encryptors, after the contractor's facility has met the DD Form 254 requirements:

- Communication link to Government systems and data as required for testing. The Government will supply the communications link and any required cryptographic equipment. The contractor is responsible for all routers, switches, etc. on its side of the interface.
- Communications link to FBI WAN for on-site Government access to email services and network.

11.3 Government Furnished Information:

- VCF IOC final report
- IPC and TNC definitions/descriptions/interfaces
- Non-commercial compliance and reference documents listed in this SOW
- Access to test data by TBS (*contractor to provide need dates*)
- Legacy system Interface Control Documents
- SUS Patch Management Roadmap
- Patch Management Overview
- Check for Available Patches
- Enclave/System Manager Approval
- Test Patch
- Deploy Patch
- Backout/Recovery and Reporting
- Notification Procedures

12. Packaging, Packing, and Shipping Instructions

The contractor shall ensure that all items are preserved, packaged, packed and marked in accordance with best commercial practices to meet the packing requirements of the carrier and to ensure safe and timely delivery at the intended destination. All data and correspondence submitted shall reference:

1. The CIO-SP2*i* Task Order Authorization Number
2. The NITAAC Tracking Number
3. The government end user agency
4. The name of the COTR

Containers shall be clearly marked as follows:

1. Name of contractor
2. The CIO-SP2*i* Task Order Authorization Number
3. The NITAAC Tracking Number
4. Description of items contained therein
5. Consignee(s) name and address

All commercial shipments to the JEH Building shall follow the instructions contained defined in the FBI Instruction: Commercial Delivery Instructions J. Edgar Hoover (JEH) FBI Building and Washington Field Office (WFO) dated 27 Dec 2000.

All shipments to Clarksburg, WV facility shall be addressed to:

1000 Custer Hollow Road
Clarksburg, WV 26306
Attn: Data Center

Shipping instructions for the Washington D.C. Data Center are located in the Commercial Delivery Instructions J. Edgar Hoover (JEH) FBI Building and Washington Field Office (WFO) dated 27 Dec 2000. Plan on an additional week beyond shipping time for commercial deliveries.

13. Inspection and Acceptance Criteria

Final inspection and acceptance of all work performed, reports and other deliverables will be performed at the place of delivery.

14. Accounting and Appropriation Data

Note that funds are not presently available for award of a contract at the time of issuance of this solicitation document. Therefore, the Government's intent to award a contract under this solicitation is contingent upon the availability of appropriated funds. No legal liability on the part of the Government can be incurred if an award is not made.

15. Other Pertinent Information or Special Considerations

15.1 Performance Criteria

The Award Fee Plan (AFP) defines the opportunity the Contractor has to earn fee commensurate with demonstrated performance. The Award Fee Plan has been developed to incentivize continuous Contractor responsiveness to program priorities and place an emphasis on quality program and technical management as well as cost and schedule savings. The Government will pay the Contractor an award fee for satisfactory or better performance. Notionally, the government anticipates capping the award fee pool for the development effort at 12% of development costs. Development costs are all costs incurred prior to each Phase Delivery Acceptance, not including equipment and "other direct costs". The award fee earned by the Contractor will be determined following successful completion of each Phase milestone event including: Initial Baseline Review (IBR), Critical Design Review (CDR), Operational Readiness Review (ORR), and Delivery Acceptance Review (DAR) for each phase. The government, at its sole discretion, reserves the right to roll unearned fee into any subsequent period within Phase; or into any subsequent Phase that has been contractually executed. Additional fee may be awarded for accelerated delivery as defined in Section 3 of the Award Fee Plan, Attachment 11. The fee structure is intended to encourage strong performance by the contractor in the highest risk areas. For more details on the government's perceived risk in each phase, accelerated delivery schedule, and the evaluation criteria for establishing the award fee, the Award Fee Plan (AFP) is provided in Attachment 11.
The performance requirements related to Award Fee Plan section 2.5.4.2-Technical Management and Performance for each task are contained in Table 15.1-1 below. Table 15.1-2 contains mandatory SLA content.

Table 15.1-1 Performance Requirements

Item of Interest	Desired Outcome	Performance Standard	Monitoring Method
Acquisition Objectives	Phase deployments meet SOW acquisition objectives	Deployed Phases achieve Government's stated acquisition objectives (SOW para 3.0)	Government review of planned and actual Phase content.
SENTINEL Phase Capability Performance	Phase successfully completes all verification activities including: acceptance testing, security testing, and records management testing.	SENTINEL system level acceptance testing in an operating environment at a designated FBI facility meets the functional and performance standards established in the SRS and allocated to that Phase. Record management certification and Approval to Operate are achieved.	Government assessment of Phase test data and test reports.
Systems Engineering Execution	SENTINEL successfully passes its required LCMD gates and project reviews per Phase.	Phase's LCMD control gates and project reviews successfully completed using the entrance and exit criteria established in the IMP. The Government shall be final approval authority as to a successful gate/project review event.	Government assessment of LCMD gate and project reviews.
Architecture Qualities	The SENTINEL architecture is scalable, robust, and flexible. The architecture complies with the FBI Enterprise Architecture. The architecture reflects a modular approach that embraces encapsulation of functionality. The architecture supports easy integration among components and products that were not necessarily originally designed to work together. The architecture facilitates changes to be accommodated in a manner such that changes propagate to as few other components as possible.	100% compliance is required.	Government analysis of architecture products, modules, and interfaces to assess descriptions, definitions, attributes, use of rules and conventions for standards compliance, product consistency, communicability, and implementation viability.
Information Sharing	The architecture facilitates information sharing by using Government standard XML schema definitions where appropriate to interface with external	100% compliance is required.	Government analysis of architecture, modules, and interfaces.

Item of Interest	Desired Outcome	Performance Standard	Monitoring Method
	systems that will support the rapid exchange of electronic information with External Agencies. The architecture has a single point of access to investigative information within the FBI. The architecture supports common standards for information sharing, as delineated by the contractor.		
Phase data migration	All necessary data is migrated from each legacy system. Each migrated data set is complete and accurate. "Data" not meeting the SENTINEL data standards is flagged and provided to the Government for action.	100% compliance is required.	Government review and independent verification and validation of data migration test results.
Phase schedule and file plan data	Government approved, complete and accurate schedule and file plan data are loaded in the system. Delivered records management capability is fully operational.	100% compliance is required.	Government review of product. Government monitoring of system level tests. Independent verification and validation results review.
Phase technical data package	The technical data package is complete and accurate, reflecting the as delivered system configuration. Documentation for the system administrators is complete, accurate and easy to use.	100% compliance is required.	Government review of contractor audit records. Government review of configuration audits. Independent verification and validation. Government Functional and Physical Configuration Audits.
O&M Training	System Administrators, privileged users, and help desk operators shall receive training and training materials appropriate for their intended use of the system.	Training materials are clear, concise, correct, and use color diagrams to lead the user through the learning process. Users can perform all routine tasks at the completion of training (includes a combination of classroom training, on-the-job training, and reading of baseline procedures, manuals, and guidebooks).	Government review of training materials. Government monitoring of courses. Government monitoring of student evaluations.
Service Level	The system is operated and	100% compliance is required.	Review of: trouble tickets,

Item of Interest	Desired Outcome	Performance Standard	Monitoring Method
Agreements	maintained at the levels specified in the Government approved Service Level Agreement.		contractor maintenance logs, and contractor incident tracking reports.
User Training	System users shall receive training and training materials appropriate for their intended use of the system.	Training materials are clear, concise, correct, and use color diagrams to lead the user through the learning process. System users can perform all routine operations at the completion of training (includes a combination of classroom training, on-line training, and reading of guidebooks).	Government review of training materials. Government monitoring of courses. Government monitoring of student evaluations.
Organizational Change Management	User Communities – agents, analysts, professional staff, O&M staff are well informed of and accept each Phase's deployed capabilities.	User Communities – agents, analysts, professional staff, O&M staff, are participants during SENTINEL development, deployment, and employment. Their concerns and issues are responsively and effectively addressed	SENTINEL's User Advocate Team assessment and Deployment Readiness Review results
Users employment of Phase's capability	User Communities – agents, analysts, professional staff, O&M staff are well trained and can effectively and efficiently use a Phase's set of capabilities	Users self-report work productivity improvement.	SENTINEL's User Advocate Team assessment based on Field Offices and Hq inputs.

Table 15.1-2 Mandatory SLA Content

Item of Interest	Desired Outcome	Performance Standard	Monitoring Method
Updates and Patches	Updates and patches are implemented within one week of approval by the Configuration Control Board.	100% compliance is required unless a Government waiver of the requirement is approved.	Audit of configuration management logs. Monitoring of operations and maintenance activities.
Maintaining System Security	System security is maintained at the certified level using the baselined security documentation. The security documentation is kept up to date using the baselined configuration management procedures to reflect any security related changes to the system.	100% compliance is required.	Review of the security documentation. Audit of configuration management logs.
Asset	All assets are accounted for	Assets changes are logged	Audit of inventory records

Item of Interest	Desired Outcome	Performance Standard	Monitoring Method
Accounting and Inventory	and an up to date inventory is maintained.	within 24 hours of arrival/departure.	and inventory.
Periodic Maintenance	Periodic Maintenance for hardware shall not exceed 2 hours/week	100% compliance is required.	Audit of maintenance logs
Vendor Response Time	The ITOD's Data Center Unit (DCU) requires a one hour response time for vendor support	100% compliance is required.	
Problem Ticket/System Defect Response time	EOC response timelines are met/supported	Critical = Acknowledged in 15 minutes, problem resolved within 2 days High = Acknowledged in 24 hours, problem resolved within 4 days Medium = Acknowledged in 48 hours, problem resolved within 5 days Low = Acknowledged in 72 hours, problem resolved within 6 days	Review of ServiceCenter™ logs

15.2 Organizational Conflict of Interest (OCI) Mitigation Plans

Every contractor or subcontractor who submits an offer as a prime contractor or as a member of a contractor teaming arrangement shall review and comply with FAR Subpart 9.5. Each of the items listed below shall be specifically addressed corresponding to the unique numeric designation.

1. Organization charts showing the company's corporate structure and highlight elements of the company participating in the contract.
2. Demonstrate how the elements performing the proposed effort will be isolated from the remainder of the company.
3. Describe how information, whether in hard copy or electronic media, will be stored and destroyed in order to preclude a transfer of information.
4. Describe how networks and servers will be protected to prevent unauthorized transfer of information.
5. Describe management reporting chains in sufficient detail to demonstrate that the proposed effort and decisions related to the effort will be isolated from the remainder of the company.
6. Address how your company will preclude a perception of impaired objectivity.
7. Provide information to indicate if the organizational elements performing the proposed effort will be geographically or physically separated from the remainder of the company.
8. Describe techniques your company will employ to mitigate the perception that you will favor your own products or services.
9. Describe the process in which the government will have insight or oversight of key processes.
10. Describe any situation in which management outside the mitigated organization will have access to key decisions for which the mitigated organization is responsible.
11. Provide all documents that your employees are required to sign indicating, which employees are required and how often the requirement is.
12. Describe the process for reassigning personnel, including subcontractors, from one assignment to another, include restrictions.

13. Describe the process for employees that leave your employment and any control you exercise over their future employment, particularly as it relates to OCI and non-disclosure.
14. Describe any OCI training your employees are offered and or mandated, along with the timing (before or after starting work on a government contract) frequency, length and content of such training.
15. Describe if your company conducts self-audits and if they will be made available to the government.
16. Describe the proposed process and timeline for submitting, and obtaining the approval by the Contracting Officer, of the OCI Mitigation Plans for any and all subcontractors added to the contract post award that were not included in the OCI Mitigation Plans submitted as part of the contractor's proposal.

To enable the Government to fairly evaluate the proposed plan, the following shall be specifically addressed:

A. Disclosure of business activities of your company, your affiliates, your team members and affiliates of your team members which create either a conflict of interest or the appearance of a conflict of interest.
B. Provide evidence of facts and circumstances that you believe mitigate or address concerns related to the appearance and/or presence of an OCI.
C. Explain your proposed approach to mitigating the effects of any apparent or actual conflicts of interest arising out of the business activities disclosed in response to (A.) above.

The government will treat all submissions as proprietary under 18 U.S.C. §1905 and protect proposed information accordingly.

15.3 Reserve

15.4 Contractor Travel

All travel must be pre-approved by the COTR in writing and must comply with the Federal Travel Regulation.

15.5 SENTINEL Standards

15.5.1 Usability Standards (TBR):

- ISO 13407:1999 - "Human Centered Design Processes for Interactive Systems"
- ISO 11581 - "Icon Symbols and Functions"
- Microsoft GUI guidelines

15.5.2 Development Standards:

The FBI prefers use of these tools however compatible alternatives are acceptable:

- Popkin System Architect
- Popkin Integrated Reference Model Application
- AllFusion® ERwin Data Modeler

15.5.3 Operations and Maintenance Standards

The following are a list of the products and services used by ITOD:

- Peregrine's Service Center™ is utilized for Change Management, Security Access Request (SAR), SLA Tracking, and generating Trouble Tickets. It assists with the tracking and the approving of changes to the FBI's IT environment for network and baseline software changes, file changes, application software changes, etc. Recording and tracking processes for Commercial Off-the-Shelf (COTS) software is another utilized feature of Peregrine's Service Center™.

- RATIONAL (i.e. ClearQuest™, ClearCase™) is being utilized by the FBI to perform modeling, version control of software and documents, defect workflow/tracking, enhancement request workflow/tracking, testing, performance testing, and requirements tracking. This tool shall be utilized by the development team and transitioned to ITOD for O&M purposes.

- Enterprise standards (commercial software products) for network monitoring and management are listed below. The FBI prefers use of these tools. The Offeror may select comparable products provided they interface to Micromuse's Net Cool and they provide justification for the selection.

  - HP Openview (enable SNAP traps and queries)
  - NetIQ – Application Manager (server agent)
  - NetIQ – Security Manager (server agent)
  - E-Policy Orchestrator (McAfee NetShield)
  - Tripwire (server agent)
  - Navisphere (agent for EMC SAN management)
  - Micromuse Net Cool (enable SNAP traps and queries)
  - SMS Agent (agent for remote management)
  - Antigen (email antivirus) (server agent)
  - Veritas Netbackup (backup management) (server agent)
  - Infovista (performance management) (SNMP traps)
  - CiscoWorks (configuration management) (SNMP traps)
  - RSA ACE (authentication) (syslog messages)
  - Cisco Secure ACS (Cisco access control) (syslog messages)
  - Dell OpenManage Suite (Hardware Health monitoring of all Dell Servers).
  - Native Windows 2000 Server tools (e.g. Cluster Administrator, AD Users & Computers). More detailed applets used to monitor smaller pieces of the enterprise when needed.
  - NetIQ DRA (3rd party tool used in place of Active Directory Users and Computers, used more for troubleshooting than monitoring).

  At the time of contract award through the period of performance, in the event that enterprise standard software packages for network monitoring and management encounter changes, the vendor is expected to factor into the contract operations and maintenance the need to train their technicians accordingly to provide the same level of response to all software changes at no additional charge.

- The FBI's current VIRUS Protection Software shall be used to the extent possible.

- The SENTINEL client "applications" shall run on FBI approved desktops.

15.6 Government Space at Contractor Facility

Although some work will be accomplished at FBI facilities, the primary site for work associated with this Task Order shall be the contractor's facility. The contractor shall support frequent short notice meetings and briefings at FBI Headquarters and other locations in the Washington, D.C. metropolitan area.

The contractor provided facility shall contain sufficient floor space to house contractor personnel, government personnel (15), computer systems and components. The facility shall support both Unclassified/For Official Use Only (FOUO) and Secret. The two enclaves shall be separate and distinct

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00163 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.104

from each other as well as any corporate network. It is anticipated that the activities such as document development, purchasing, and program management will be housed on the Unclassified/FOUO network. The Secret network shall host the development, test, integration of the new system and the FBINet for communications, email, and document exchange.

15.7 Installation Support

The Government will provide the operational and backup facilities. Workspaces for TBS *(offeror to supply requirement as part of proposal)* operations and maintenance personnel will be provided. The contractor shall be responsible for all cable and cable pulling activities from the agreed to interface to and between the delivered equipment. Standards for the facilities are contained in the ITOD Data Unit, Equipment Installation Standards and ITOD Data Unit, Equipment Installation Standards (Clarksburg, West Virginia)documents.

15.8 Key Personnel

Key Personnel considered essential to the performance of this Task Order are:

- Task Order Program Manager
- Task Order Deputy Program Manager
- Task Order System Chief Engineering and Architecture Manager
- Task Order System Test Manager
- Task Order Certified Records Manager *
- Task Order Security Engineering Manager
- Task Order Organizational Change Training and Transition Manager

*Certification via Institute of Certified Records Manager. Equivalent qualifications may be considered.

Key Personnel Qualifications are provided at SOW Attachment 4-Key Personnel Duties and Qualifications.

15.9 Software Licenses

If development tools are proposed that require licenses/seats foı Government use, 15 seats for Government use shall be purchased.

15.10 Development Environment

If not available through an existing FBI enterprise license agreement, hardware and software used in the development of the system shall be procured under this contract and delivered to the Government at the completion of the contract. All licenses and warranties purchased under this contract shall be transferable and shall be transferred to the Government at the completion of the contract or upon Government request.

The development environment includes all strings used to develop and operate SENTINEL including unclassified and classified development, integration and test, staging, operations, backup, and training strings.

15.11 Applets, Plug-ins and Other Applications Planned for FBINet

Any applet, plug-in or other applications that will be pushed to or reside on FBINet clients require Government approval. Descriptions of any proposed applet, plug-in or other applications shall be identified to the Government no later than PDR.

15.12 Software Engineering Institute (SEI™[2]) Capability Maturity Model Integration (CMMI®[3]) Level 3 Requirement

The contractor, including all organizations and subcontractors that will be contributing a minimum of 10% of the total SENTINEL level of effort developing or integrating software, shall perform the task order activities in accordance with the processes assessed at an SEI CMMI (or equivalent) Level 3 as presented in the proposal. The Government reserves the right to conduct independent assessments during the period of performance to verify compliance with established processes. In the event that the contractor provided a risk mitigation plan, an implementation plan, and a schedule for achieving full compliance in lieu of an existing CMMI Level 3 assessment, the Government reserves the right to conduct independent assessments to verify achievement of the Level 3 processes.

15.13 Vendor Contracts for Operations and Maintenance

The contractor and the Hardware/Software Vendors must have agreements that specifies the following: Local service personnel availability and backup resources; test equipment and services; provide all current and revised test equipment (i.e. hardware, software, and firmware); maintenance and escalation plans during bi-annual meetings between the FBI and the contractor; the ability to work with other vendors for solutions when necessary; the ability for the original equipment manufacturer to inspect government equipment for mandatory engineering change orders to upgrade equipment; vendor provided computer engineers/technicians that have expert level experience in maintaining the same or similar equipment. Ensure that parts are included as a mandatory requirement for hardware maintenance.

15.14 Mandatory Patch Management Procedures

The Software Update Services (SUS) Patch Management Process is contained in the SUS Patch Management Process document. The SUS Roadmap and Patch Management Overview documents provide a description of the Patch Management Process for implementing software patches within any network in the FBI headquarters. This guidance shall be followed when conducting patch management on any SENTINEL operational system. Process documents are:

- SUS Patch Management Process
- Check for Available Patches
- Enclave/System Manager Approval
- Test Patch
- Deploy Patch
- Backout/Recovery and Reporting
- Notification Procedures
- SUS Roadmap
- Patch Management Overview

15.15 Release Information – Publications by Contractor Personnel

The Federal Bureau of Investigation (FBI) specifically requires that Contractors shall not divulge, publish, or disclose information or produce material acquired as or derived from the performance of their duties.

---

[2] (SM) SEI is a service mark of Carnegie Mellon University

[3] ® CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

For purposes of this Clause, "Information" shall include but not be limited to: in any media or all media including on the web or web sites; publications, studies, books, theses, photographs, films or public announcements, press releases describing any part of the subject matter of this contract or any phase of any program hereunder, except to the extent such is:

(i) already known to the Contractor prior to the commencement of the contract
(ii) required by law, regulation, subpoena or government or judicial order to be disclosed, including the Freedom of Information Act.

No release of information shall be made without the prior written consent of the Office of Public Affairs and the Contracting Officer. The contractor and author are warned that disclosure is not without potential consequences. The FBI will make every effort to review proposed publications in a timely manner to accommodate these and other publications.

Where appropriate, in accordance with established academic publishing practices, the FBI reserves the right to author/co-author any publication derived from this contract.

These obligations do not cease upon completion of the contract.

15.16 Privacy Act

All contractors and subcontractors shall comply with 5 USC 552a(m) of the Privacy Act which reads as follows:

"(m) Government contractors

(1) When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i)[4] of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

(2) A consumer reporting agency to which a record is disclosed under Section 3711 (e) of Title 31 shall not be considered a contractor for the purposes of this section"

16. Post-Award Administration

The Government will monitor the contract performance using the contractor provided IMP and IMS. Milestones and work activities along with LCMD control gates and reviews shall be monitored following the performance criteria in the Award Fee Plan at Attachment 11.

Critical Path Management (CPM) will be used as the primary schedule and cost control mechanism. Progress will be measured using Earned Value Management (EVM). The Government will be using Microsoft Project 2003 Professional and Metier's WorkLenz™5 software package to monitor schedule and earned value performance and report on that performance up through the OMB Exhibit 300 reporting cycle. The contractor shall be required to submit data at least monthly in electronic formats suitable for uploading into the Government's MS Project and WorkLenz project files.

[4] Section (i) has criminal penalties – misdemeanor and $5,000 fine

The Government will complete award fee evaluations following process and schedule defined in the Award Fee Plan in Attachment 11.

In accordance with NIH SP2 requirements, the Government will complete Past Performance Evaluations at least annually and at the end of the task.

17. Evaluation Criteria

Award of the SENTINEL Task Order will be made to the Contractor whose proposal, conforming to this solicitation, is determined to be the best value to the Government using the "Best Value" process as defined in FAR 15.101-1. This process permits trade-offs between cost or price and non-cost considerations and allows the Government to accept other than the lowest priced proposal. In such an occurrence, the perceived benefits of the higher priced proposals shall merit the additional cost.

The Technical Approach and Management Approach evaluation items are of equal importance. Both Technical and Management Approach items, individually, are more important than the Past Performance item. The Security Approach and OCI Mitigation evaluation items will be assessed on a Pass/Fail basis. Failure of either of these items may result in the offer being removed from consideration. The Past Performance, Technical Approach and Management Approach evaluation items, when combined, are significantly more important than Cost. In the case of essentially equal and acceptable evaluation of Past Performance, Technical Approach and Management Approach, Cost will assume greater importance, and may become the determinative factor for making award.

Note that funds are not presently available for award of a contract at the time of issuance of this solicitation document. Therefore, the Government's intent to award a contract under this solicitation is contingent upon the availability of appropriated funds. No legal liability on the part of the Government can be incurred if an award is not made. Award will be made to the Offeror proposing the solution most advantageous to the Government based upon an integrated assessment of the evaluation Items and Factors listed below, cost and other factors considered. The SENTINEL evaluation criteria for award are:

I. Past Performance Item

This evaluation item examines the quality of the Offeror's past performance on programs that are similar in size, scope and technological and managerial complexity to the SENTINEL program. The Government will evaluate the quality of the Offeror's past performance and reserves the right to seek out past performance information in addition to that provided in the proposal, from any and all sources both inside and outside of the Government, and to use the information received in the evaluation of past performance. These cited programs must be appropriately recent and relevant in order to receive favorable consideration. In determining the rating for the past performance evaluation factor, the Government will give greater consideration to the Offeror's performance under the contracts which the Government feels are most relevant to SENTINEL. This item includes assessments of Technical Past Performance, Management Past Performance, and a Demonstration of one of the fielded systems cited in the Offeror's Past Performance volume.

Factor 1: Technical Performance
This factor evaluates the quality of the Offeror's technical performance on recent and relevant programs. The factor addresses the adequacy of the Offeror's demonstrated capability in developing and deploying technology that is applicable to the SENTINEL program. Included in this factor will be an assessment of the Offeror's success in meeting program performance requirements using a phased development approach, integrating COTS/GOTS products at the enterprise level, and migrating legacy data and applications.

Factor 2: Management Performance
This factor evaluates the quality of past management performance on recent and relevant programs. The factor addresses the adequacy of the Offeror's demonstrated performance in

managing and executing recent and relevant programs that are applicable to the SENTINEL program. Included in this factor will be an assessment of success in meeting schedule requirements, cost control requirements and program planning and execution.

Factor 3: Past Performance System Demonstration
This factor evaluates the quality of the performance of a deployed system that the Offeror has developed and believes to be of relevance to the proposed SENTINEL functionality. Included in this factor will be an assessment of the quality of the deployed system's implementation of key SENTINEL functionality, to include any or all of the following:

- Case Management
- Document Management
- Document Authoring
- Evidence Management
- Records Management Application (RMA) or Electronic Records Keeping (ERK)
- Security (Discretionary Access Control, Role-Based Access Control)
- Workflow

II. Technical Approach Item

This evaluation item examines the quality of the Offeror's proposed technical approach to meeting the SENTINEL performance requirements. This item includes assessments of the quality of the Offeror's proposed SENTINEL solution and of their phased development approach.

Factor 1: Proposed Technical Solution
This factor evaluates the quality of the Offeror's technical solution as evidenced by their description of an adequate systems architecture and system design. The factor also evaluates the sufficiency of the proposed COTS/GOTS selection approach and identification, as well as the adequacy of the proposed solution's scalability, maintainability and security attributes. This factor also addresses the quality of the Offeror's approach to legacy data migration and legacy application transition.

Factor 2: Phase Development Approach
This factor evaluates the quality of the Offeror's phased development approach as evidenced by their description of an adequate system development approach. The factor also evaluates the sufficiency of the proposed Integration and Test approach, as well as the adequacy of the proposed technical deployment approach and pre-FOC Operations and Maintenance strategy.

III. Management Approach Item

This evaluation item examines the quality of the Offeror's proposed management approach for executing the SENTINEL design, development, integration and test, deployment, and operations and maintenance. This item includes assessments the quality of the Offeror's Executive Overview, proposed program organization, Systems Engineering approach, appropriateness and quality of their Team composition, and quality of the organizational change management strategy.

Factor 1: Executive Overview (Oral Briefing)
This factor evaluates the Offeror's understanding and overall approach to satisfying the requirements of the TORP. It includes an assessment of the Offeror's proposal strengths and capabilities, excluding cost/price, as well as the proposed solution to managing technical processes.

Factor 2: Program Organization
This factor evaluates the quality of the Offeror's proposed strategy for managing the SENTINEL program development activity. Included in this assessment is an evaluation of the quality of the

Offeror's proposed Integrated Master Plan, the adequacy and realism of their proposed program schedule, the adequacy of the Offeror's implementation and traceability of SOW requirements, their proposed staffing approach and the adequacy of the Offeror's strategy for identifying, mitigating and managing SENTINEL programmatic and technical risk.

Factor 3: Systems Engineering
This factor evaluates the quality of the Offeror's proposed systems engineering methodology and the appropriateness of the tailoring of that process for the SENTINEL program. It also evaluates the adequacy of the Offeror's systems engineering processes as they are applied to their proposed solution.

Factor 4: Team Composition
This factor evaluates the quality of the Offeror's proposed corporate skills and abilities represented on their proposed SENTINEL team, and the appropriateness of their team composition in light of the stated goals and objectives of the SENTINEL acquisition. Included in this factor is an assessment of the qualifications of the Offeror's proposed Key Personnel, the ability of their Team organization and roles and responsibilities to adequately ensure an efficient and effective fit within the overall government organization, and of the adequacy and appropriateness of the proposed Team's domain knowledge.

Factor 5: Organizational Change Management
This factor evaluates the quality and effectiveness of the Offeror's proposed Organizational Change Management (OCM) strategy. Included in this factor is an evaluation of the Offeror's proposed methodology and approach to ensuring user acceptance through ongoing communications, program advocacy and marketing and the development and deployment of training. Also included in this factor is an assessment of the Offeror's transformation approach, which must demonstrate an adequate understanding of the business changes associated with SENTINEL and describe a plan for mitigation of user resistance.

IV. Security Approach Item (Pass/Fail)

This evaluation item examines the quality of the Offeror's proposed approach for meeting the SENTINEL security requirements. This evaluation item encompasses the evaluation of four factors for award: Personnel Security, Infrastructure Security, Lifecycle Security, and Acquisition Risk Assessment. Evaluation of these factors is Pass/Fail. Failure to meet these the standards of these evaluation factors may result in the Offeror's proposal no longer being considered for award.

Factor 1: Personnel Security
The Personnel Security Factor evaluates the Offeror's compliance with personnel security requirements for the SENTINEL program. Included in this evaluation will be a verification of the status of the proposed cleared personnel at contract award in accordance with the appropriate FBI Security policies and the SENTINEL SOW, the Offeror's willingness to participate in the FBI's polygraph program, as well as an assessment of the adequacy of the Offeror's proposed plan of action for augmenting their cleared labor pool beginning at contract award to meet SENTINEL requirements for appropriately cleared personnel.

Factor 2: Infrastructure Security
The Infrastructure Security Factor evaluates the Offeror's compliance with infrastructure security requirements necessary to support the SENTINEL program. Included in this evaluation will be a verification of the status of the proposed accredited Offeror facilities at contract award in accordance with the appropriate FBI Security policies and the SENTINEL SOW. This factor will evaluate the adequacy of the Offeror's plan for providing an FBI-accredited development environment that meets the facility requirements of the SENTINEL SOW at the time of contract award, or a plan for how these requirements will be met. This factor also includes an assessment of the Offeror's plan for complying with FBI security requirements for the processing of

SENTINEL program data on automated information systems within the Offeror's development environment.

Factor 3: Lifecycle Security

The Lifecycle Security Factor evaluates the quality of the Offeror's plan for identifying and incorporating appropriate security measures throughout the SENTINEL program lifecycle. Included in this evaluation will be an assessment of the Offeror's proposed approach for maintaining compliance with, and staying abreast of all appropriate FBI security policies and directives. This includes the corporate commitment for staffing SENTINEL tasks with appropriately cleared personnel, maintaining accredited facilities, and implementing a robust security management plan for teammates and subcontractors.

Factor 4: Acquisition Risk Assessment

The Acquisition Risk Assessment Factor evaluates the risk posed to the government by the Offeror of the SENTINEL acquisition. Included in this evaluation will be an assessment of the Offeror's Certificate Pertaining to Foreign Interests (SF 328) and Key Management Personnel List (KMPL), particularly the impact of any Foreign Ownership Control or Influence (FOCI) on their organization or activities, or the organization or activities of a subcontractor.

V. Organization Conflict of Interest Item (Pass/Fail)

The Organizational Conflict of Interest (OCI) Mitigation Item evaluates the Offeror's proposed plan for mitigating any and all real or perceived organizational conflicts of interest. The evaluation criterion is met when the Offeror's OCI Mitigation Plan describes an acceptable approach to identifying, avoiding, and mitigating organizational conflicts of interest. Evaluation of this item is Pass/Fail. Failure to meet this criterion may result in the Offeror's proposal no longer being considered for award.

VI. Cost/Price Item

The Cost Item evaluates the Offeror's proposed cost for realism, reasonableness and completeness. The objective of proposal cost analysis is to ensure that the final agreed-to price is fair and reasonable. Cost information may be provided to members of the Non-Cost evaluation team in accordance with agency procedures in order to provide greater expertise to the Cost evaluation team. The Cost evaluation process does not result in a qualitative rating, as does the non-cost evaluation. Rather, the Offeror's proposed cost is analyzed and any noted discrepancies in cost realism, cost reasonableness and cost completeness are noted and are communicated to the SSA during the SSET's Award Recommendation Briefing.

Factor 1: Cost Realism

The Cost Realism evaluation includes a review of the technical and management volumes and Offeror Bases of Estimate (BOEs) to determine if these approaches, and their corresponding cost estimates, are realistic for the work to be performed, reflect an understanding of the requirements, are consistent between the various elements of the proposal, and if the proposal can executed for the proposed cost.

Factor 2: Cost Reasonableness

Cost Reasonableness is assessed by reviewing the proposal Basis of Estimates (BOEs) to determine the confidence of the estimating methods used to substantiate the proposed costs. According to FAR 31.201.1, an Offeror may use any generally accepted estimating method that is equitable and consistently applied. Normally, adequate price competition establishes price reasonableness FAR 15.403-1 c.1.

Factor 3: Cost Completeness

Cost/price proposals shall be evaluated for completeness by assessing the responsiveness of the Offeror to the solicitation requirements. For the cost data to be complete, the Offeror must provide all data that is necessary to support the offer.

18. Data Item Descriptions

Data item descriptions are located in the FBI LCMD Appendix H and the FBI Certification and Accreditation Handbook except as noted below. In the event that a description is provided in the SOW and in one of the two referenced documents, the SOW description shall take precedence.

18.1 TASK ORDER MANAGEMENT PLAN 56
18.2 IN PROGRESS REVIEW REPORT (MONTHLY) 58
18.4 CONTRACT FUNDS STATUS REPORT 59
18.5 EARNED VALUE MANAGEMENT SYSTEM (EVMS) REPORT 60
18.6 RISK MANAGEMENT PLAN 64
18.7 DEFECT REPORTS 66
18.8 MEASUREMENT PLAN 67
18.9 MEASUREMENT REPORT 70
18.10 COMMUNICATIONS PLAN 71
18.11 TRAVEL PLAN 72
18.12 EOC MEMORANDUM OF UNDERSTANDING 73
18.13 RISK ASSESSMENT (DELIVERED TWICE MONTHLY) 75
18.14 INTEGRATED MASTER SCHEDULE (WEEKLY) 76
18.18 DATA ACCESSION LIST 81
18.25 DESIGN CONCEPT DESCRIPTION AND ARCHITECTURE 81
18.36 SERVICE LEVEL AGREEMENT (SLA) 82
18.39 DATA MIGRATION PLAN 83
18.40 EOC OPERATIONAL SUPPORT REQUIREMENTS DOCUMENT OF NEW SYSTEMS 84
18.41 DCU04 REQUEST FOR DATA CENTER ACCESS 91
18.42 DCU05 REQUEST FOR DATA CENTER EQUIPMENT INSTALLATION 92
18.53 TECHNICAL MANUAL (NON-COMMERCIAL HW ONLY) 93
18.65 PRODUCT (CSCI'S) 93
18.66 LOGICAL DATA MODEL 93
18.68 O&M PROCEDURES 93
18.69 O&M TRANSITION PLAN 94
18.70 SENTINEL STAKEHOLDER AND ORGANIZATIONAL RISK ASSESSMENT. 96
18.71 ORGANIZATION IMPACT ASSESSMENT (OIA) 96

18.76 AGENDAS, BRIEFINGS, MEETING MINUTES 96

18.77 WORKFORCE TRANSFORMATION STRATEGY AND PLAN..... 96

18.78 INTEGRATED MASTER PLAN..... 96

18.79 TRAINING STRATEGY AND PLAN 96

18.80 TRAINING ADMINISTRATION REPORT 96

18.81 DELIVERY ACCEPTANCE REPORT 96

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00172 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.113

18.1 Task Order Management Plan

This is the first plan for the project. The Task Order Management Plan (TOMP) provides high-level planning information and is supplemented by other, more detailed planning documents as the project proceeds through its life cycle.

1.0 Introduction

1.1 Document Overview
A Document Overview section shall summarize the purpose and contents of this document.

1.2 Program Overview
The Program Overview shall identify the name of the project and it shall identify the FBI is the acquiring entity. The Program Overview shall briefly state the purpose of the project.

2.0 Referenced Documents

This section shall list the number, title, revision, date, and originating organization of all documents referenced in this document.

3.0 Program Requirements and Objectives

This section identifies the system requirements and project deliverables.

Identify system requirements in priority order. Reference to the System Requirement Document is acceptable. Identify driving operational need dates or ties to external milestones, which may influence the structure and scope of the project. Identify the capacity that must be obtained to meet operational requirements.

List those items that the project is expected to deliver or place into operations. This may include functional capabilities, support infrastructure, number of units, documentation, and training.

4.0 Organizations

Provide a list of organizations that will be involved in the project. Identify the organizations including subcontractors, the scope and amount of effort that each organization must contribute by Phase, SOW task and subtask, and the Point of Contact (POC) in each organization. Provide a Key Management Personnel List (KPML).

5.0 Program Monitoring and Control

This section defines level of monitoring and control that will be implemented on the project.

5.1 Level of Configuration Management

Describe the techniques to ensure configuration management.

5.2 Level of Reporting and Monitoring

Describe processes to be used to monitor and report on project status and risk. Describe the Earned Value Management process to be applied on the project. Describe the measurement program. Describe the readiness planning and review process for the development and its assorted documentation based on the project level reviews and control gates defined in the SOW.

5.3 Quality Assuranee

Describe how quality practices will be implemented, assessed, and monitored. Describe the metrics that will be used to monitor the success of the project as it moves through its life cycle.

6.0 Security

Describe the security process that will be implemented on the project. Define how system security is to be addressed, including accordance with the Systems Engineering Management Plan (SEMP). Describe any special personnel security considerations of the project.

7.0 Notes

This section shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A. Appendices

Appendices may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.).

18.2 In Progress Review Report (monthly)

The In Progress Review Report is the organized documentation of proceedings of the monthly In Progress Review. The report is a compilation of briefings, handouts, and action items given at the review. Contractor formatting of briefings, handouts, and action item lists is acceptable provided that Government has not made prior restrictions in the statement of work or other data item descriptions. Contractor formatting of the report is acceptable. The In Progress Review Report shall be delivered to the Government in a Government-approved electronic format. The content of the In Progress Review Report shall include the following information in the order specified:

1. Title page
2. Brief statement (no more than one page) by the program manager summarizing the state and issues facing the program
3. Table of Contents
4. Listing of pages in the report that were changed (additions, deletions, or modification) from what was presented or distributed at the Review and a description of each change (e.g., if 5 changes were made on a page, each change must be described). Changes must be indicated on the affected page. (It is the expectation that there will be few, if any, changes between the review and the delivery of the report, and that any changes be significant.)
5. In Progress Review Action Item List (to include date opened, action, assignee, status, and date closed)
6. Required topical summaries (each summary listed in table of contents):
    - Earned value
    - Schedule
    - Funding and obligations
    - Subcontracts
    - Risks
    - Program and risk management metrics as required by the Measurement Plan
    - Quality assurance
    - Configuration management
    - Security management applied to task order
    - Staffing plan
    - Phase Development Status
    - Operations and Maintenance Status
    - OCM Status
    -
7. Other topics (each topic listed in the table of contents)

IPR briefing charts are to be provided two working days in advance of the meeting. The IPR Report is to be delivered within 3 working days following the meeting.

18.4 Contract Funds Status Report

The contractor will complete DD Form 1586, Contract Funds Status Report, subject to the latest available version of the Contract Funds Status Report Data Item Description DI-MGMT-81468.

18.5 Earned Value Management System (EVMS) Report

Earned Value Management System (EVMS Report)	Item Number: 18.5
	Revision #: R01
	Effective Date: 05-27-04

Use

This written document and the associated electronic deliverable provide detailed earned value management system (EVMS) information on the combined cost, schedule, and earned value performance through the proceeding Gregorian calendar month against a project's EVMS Baseline. The information is clearly differentiated so as to provide visibility of the project's performance as a whole against the total EVMS Baseline and the project's performance against the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology.

Interrelationship

The written document and the associated electronic deliverable are delivered to the Program Manager and the Contracting Officer (if the project is part of a contract) with the EVMS Plan, EVMS Implementation Plan (as required), Work Breakdown Structure (WBS), Integrated Master Schedule (IMS), Control Account Funding/Spend Plans, Work Authorization Document(s), Subcontractor Management Plan, EVMS Baseline, and Updated Risk Assessment as required in the Program Plan and/or Contract Statement of Work as appropriate.

Preparation information

Preparation of the written EVMS Status report

A Written EVMS Status Report will be prepared and submitted (typically by the 15th of the following month) that summarizes the EVMS performance through the end of the month immediately preceding the report.

The EVMS parameters reported are generally based on the cumulative Budgeted Cost of Work Scheduled (BCWS), Budgeted Cost of Work Preformed (BCWP), and Actual Cost of Work Performed (ACWP) to date. BCWS and BCWP data shall be budgeted and captured at the lowest available level of the EVMS Baseline, which is typically at the work package level, and rolled up to level 1 of the WBS. ACWP shall be budgeted and captured at the lowest available Control Account level of the WBS and rolled up to level 1 of the WBS.

The report shall be addressed to the Program Manager and, if appropriate, the Contracting Officer. Program stakeholders that will have access to the report include:

- The Program Manager
- The Contracting Officer
- Designated Members of the Govern ment's Program Management Team, including contracted support staff.
- FBI Executives
- All appropriate external stakeholders, including OMB.

1.0 Introduction

The introduction to the report will identify the approval or draft dates of the EVMS baseline being reported against and identify any approved Change Requests that may have been used to modify the Baseline since the last report. The report follows with the 6 sections identified below.

2.0 EVMS Graphs

Two graphs will be presented that show the BCWS, BCWP, ACWP, EAC1, and EAC2 at WBS Level 1, as monetary figures (y-axis) against Gregorian calendar months (x-axis). One graph shall be for the whole EVMS Baseline. The second graph shall be for the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology.

3.0 Historical Tables of Summary EVMS Parameters

Two tables of summary EVMS parameters for the last 6 months shall be presented. Each table shall include BCWS, BCWP, ACWP, VAC1, VAC2, CV, CPI, SV, and SPI at WBS level 1. One table shall be for the whole EVMS Baseline. The second table shall be for the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology.

4.0 Historical Tables of Summary Work Package Status

Two tables showing a summary of the status of EVMS deliverables (work packages), by calendar month, from project start through the current month shall be presented. For each calendar month since project inception through the current month being reported on, each table should list:

- The total number of deliverables due to date (to have been started by the end of the month)
- The total number of deliverables that are "on schedule" as of the end of the month.
- The total number of deliverables that are "late" as the end of the calendar month.
- The total number of deliverables reported as "late" in the previous month that are now completed and/or "on schedule"

One table shall be for the whole EVMS Baseline. The second table shall be for the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology.

5.0 Detailed Table of Late Deliverables/Work Packages

A single table listing each deliverable/work package that is now "late" as of the end of the calendar month shall be presented. The information for each deliverable shall contain the following information:

- The calendar month that the deliverable/work package was due to have been started or finished
- The WBS Number
- The responsible party
- The name/title of the deliverable/work package

- The reason that the deliverable/work package is late (either "Late Start" or "Late Finish".)
- The methodology being used to measure work package value (E. G. LOE, 0/100, 20/80, or 50/50).

6.0 Narrative Analyses

This section shall provide two narrative analyses of EVMS performance to date. One narrative analysis shall be for the whole EVMS Baseline. The second narrative analysis shall be for the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology. Each narrative analysis shall be further divided into three parts. They are:

6.1 Variance Analysis

This is a narrative discussion of the cost and schedule variances at WBS level 1. The discussion includes, this month's variances, last month's variances, reasons for the variances, and what WBS level 2 items have negative cost and schedule variances.

6.2 Overall Performance

This is a short, high-level, summary discussion of the overall EVMS performance of the project. It includes short, high-level, summary recommendations on how to improve future EVMS performance (e.g. use management-by-exception techniques to focus team performance on completing the late deliverables/work packages.) It also includes a discussion of the calculated variances at completion (EAC1 and EAC2) based on CPI and a CPI/SPI combination.

6.3 Estimate at Completion

This is a short, high-level, summary discussion/prediction about whether the project will finish on time and within budget. It includes a prediction/estimate with regards to the probable project completion date and final budget requirements.

NOTE: This summary estimate on completion date and final budget is based on the professional judgment of the appropriate Program Team. There is no definitive approach to developing this section; rather this judgment incorporates common EVMS and schedule probability calculation methods available in the literature. In addition to raw, mathematical calculation results, other factors should be considered including the nature of the contract mechanisms being used (e. g. the percentage of work that is Firm Fixed Price); and the trained and experienced professional judgment of the Program Manager and his/her staff.

7.0 Table of Acronyms and Mathematical Formulas

A table or tables shall be prepared and presented that lists the all the acronyms used in the preparation of this report and all the mathematical formulas, excepting WBS roll-ups, used in calculating EVMS parameters for this report. At a minimum, the lexicon and acronyms used as well as the mathematical formulas used shall match the lexicon, acronyms, and mathematical formulas used in the version of OMB Circular A-11 that is valid as of the date the report is prepared.

8.0 Detailed Tables of Current EVMS Parameters

Tables shall be prepared and presented that list the cumulative EVMS parameters (captured and calculated) for each summary level of the WBS (including WBS levels 4, 3, 2, and 1). One table shall be for the whole EVMS Baseline. The second table shall be for the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology. At a minimum the tables shall each present the captured or calculated values for the following table columns:

- WBS
- Name/Title
- BCWS
- BCWP
- ACWP
- CV
- CPI
- SV
- SPI
- CPI/SPI
- Baseline BAC
- EAC1
- EAC2
- Estimated BAC
- Baseline Finish Date
- Estimated Finish Date

Preparation of the Electronic EVMS Data Report

An Electronic EVMS Data Report will be prepared and submitted (typically by the 15th of the following month) that supplies input data to the FBI's electronic EVMS data reporting system. The FBI's electronic EVMS reporting system utilizes Métier's WorkLenz. The data contained in the Electronic EVMS Data Report shall be prepared and submitted using Microsoft Project 2003 and Microsoft Excel 2002. Data shall be formatted to match the input requirements of Métier's WorkLenz that is current as of the date of report submittal. Data submitted electronically shall be down to and include WBS level 6 at a minimum.

18.6 Risk Management Plan

The Risk Management Plan describes the contractor processes for risk management planning and budgeting; risk identification, assessment, and analysis; risk response planning; and risk monitoring and control. Organization and content descriptions of the Risk Management Plan are as follows:

Section 1. Introduction

1.1 Purpose
(This section describes the purpose of the risk management plan.)
1.2 Scope
(This sections details the scope of the risk management plan.)
1.3 Assumptions, Constraints, and Policies
(This section describes underlying assumptions, constraints, and government and contractor policies relating to the risk management of the project.)
1.4 Referenced Documents and Standards
(This section contains the following information for any document or standard referenced with the Risk Management Plan: document identifier, title, organization/author, version number, date of publication.)

Section 2. Overview of Risk Management Process

2.1 Overview
2.2 Process and Data Flows
(As part of the description of the risk management process and data flows, this section includes the titular identification of risk management personnel and their roles and responsibilities; frequency of risk management activities; and risk management reporting requirements.)
2.3 Program Management Integration
(This section describes the extent to which project management is integrated into the risk management process.)

Section 3. Organizational Considerations

3.1 SENTINEL Organization
(This section describes how the contractor team is organized and identifies the key members of the risk management processes by name and role. An organizational chart will be included.)
3.2 Program Communications and Responsibilities
(This section describes how communications will be conducted relating to risk management processes, what responsibilities exist in communication, and how timely risk management communications will be maintained in the SENTINEL project.)
3.3 Subcontractor Responsibilities
(This section describes how subcontractors will be integrated into the risk management process, and what their roles and responsibilities will be.)

Section 4. Process Details

4.1 Identifying Risks
(This section describes the process for identifying risks.)
4.2 Analyzing Risks
(This section describes the methods for establishing the probability that a risk will occur and quantifying the impact of occurrence. The section also describes the methods determining the impact of mitigation activities associated with a risk.)
4.3 Planning to Mitigate Risks
(This section describes the methods used in planning to mitigate risks.)
4.4 Tracking and Control of Risks
(This section describes how risks will be tracked, how mitigation efforts will be assessed, and what mechanisms will be used in controlling risk.)
4.5 Summary of Methods, Tools, and Metrics
(This section summarizes the methods, tools, and metrics involved with the risk management processes.)

Section 5. Resources and Schedule of Risk Management Milestones

(This section identifies risk management milestones and describes the associated entrance and exit criteria. The section also identifies the resources to be used in achieving the milestones.)

Section 6. Documentation of Risk Information

(This section describes how risk information will be documented, managed, and accessed.)

Section 7. Methodology Associated with Changes in Scope and Funding

(This section describes the risk management methodology associated managing the project baseline in the event that project scope or funding undergoes significant change.)

18.7 Defect Reports

Government Approved Contractor Format.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00183 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.124

18.8 Measurement Plan

Government Approved Contractor Format

Contractor format must address the following elements:

- Measurement Roles, Responsibilities, and Communications
- Description of Program Information Needs
- Definition of each Measurement (detailed)* including Critical Performance Measures (CPMs) as they are established (refer to IT LCMD Appendix H for CPM content requirements)
- Data Collection and Analysis Procedures
- Measurement Evaluation Criteria for each measure
- Data reporting method

Below is a sample measure specification (source: Practical Software and System Measurement) that the contractor can tailor or replace with a suitable substitute This sample is provided to show the expected level of detail.

Measurement Information Specification

Measure Name

Information Need Description	
Information Need	What the measurement user (e.g., manager or project team member) needs to know in order to make informed decisions.
Information Category	A logical grouping of information needs that are defined in PSM to provide structure for the Information Model. PSM categories include schedule and progress, resources and cost, product size and stability, product quality, process performance, technology effectiveness, and customer satisfaction. Categories are defined in Chapter 2 of the PSM book.

Measurable Concept	
Measurable Concept	An idea for satisfying the information need by defining the entities and their attributes to be measured.

Entities and Attributes	
Relevant Entities	The object that is to be measured. Entities include process or product elements of a project such as project tasks, plans/estimates, resources, and deliverables.
Attributes	The property or characteristic of an entity that is quantified to obtain a base measure.

Base Measure Specification

Base Measures	A base measure is a measure of a single attribute defined by a specified measurement method (e.g., planned number of lines of code, cumulative cost to date). As data is collected, a value is assigned to a base measure.
Measurement Methods	The logical sequence of operations that define the counting rule to calculate each base measure.
Type of Method	The type of method used to quantify an attribute, either (1) subjective, involving human judgement, or (2) objective, using only established rules to determine numerical values.
Scale	The ordered set of values or categories that are used in the base measure.
Type of Scale	The type of the relationship between values on the scale, either: • Nominal - the measurement values are categorical, as in defects by their type. • Ordinal - the measurement values are rankings, as in assignment of defects to a severity level. • Interval - the measurement values have equal increments for equal quantities of the attribute, such as an additional cyclomatic complexity value for each additional logic path in a software unit. • Ratio - the measurement values have equal increments, beginning at zero, for equal quantities of the attribute, such as size measurement in terms of LOC.
Unit of Measurement	The standardized quantitative amount that will be counted to derive the value of the base measure, such as an hour or a line of code.

Derived Measure Specification	
Derived Measure	A measure that is derived as a function of two or more base measures.
Measurement Function	The formula that is used to calculate the derived measure.

Indicator Specification	
Indicator Description and Sample	A display of one or more measures (base and derived) to support the user in deriving information for analysis and decision making. An indicator is often displayed as a graph or chart. Include a sketch of the indicator.
Analysis Model	A process that applies decision criteria to define the behavior responses to the quantitative results of indicators.
Decision Criteria	A defined set of actions that will be taken in response to achieved quantitative values of the model.
Indicator Interpretation	A description of how the sample indicator (see sample figure in indicator description) was interpreted.

Data Collection Procedure (for each Base Measure) Complete this section for each base measure listed on the previous page.	
Frequency of Data Collection	How often data is collected.
Responsible Individual	The person who is assigned to collect the data.
Phase or Activity in which Collected	The phase or activity when the data is collected.
Tools Used in Data Collection	List any tools used to collect the data (e.g., source code analyzer).
Verification and Validation	List any V&V tests that will be run to ensure the data is complete and accurate.
Repository for Collected Data	List any tools where data is stored after it is collected (e.g., database).

Data Analysis Procedure (for each Indicator)	
Frequency of Data Reporting	How often data is reported (this may be less frequent than it is collected).
Responsible Individual	The person who is assigned to analyze data and report the results.
Phase or Activity in which Analyzed	The phase or activity when the data is analyzed.
Source of Data for Analysis	List any sources of data for this analysis.
Tools Used in Analysis	List any tools used for analysis (e.g., statistical tools).
Review, Report, or User	Document when results are reviewed and reported, along with the intended user of the results.

Additional Information	
Additional Analysis Guidance	Provide any additional guidance on variations of this measure.
Implementation Considerations	List any process or implementation requirements that are necessary for successful implementation.

18.9 Measurement Report

Government approved contractor format with the following guidance:

Provide monthly metrics reports on the metrics defined in the Measurement Plan. Provide explanations and interpretations of reported metrics data, including deviations from expected or projected values and breaches of thresholds, as well as any corrective actions being undertaken.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00187 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.128

18.10 Communications Plan

A template for a Communications Plan is provided at SOW Attachment-5 Communications Plan template. SOW Attachment-5 contains the Government's desired plan content and level of detail. The Communications Plan shall address the topics contained in the attachment.

18.11 Travel Plan

The Travel Plan is a three-month projection of all program-related travel. For each anticipated trip, the Travel Plan contains the following information: SOW task and subtask number, project phase, reason for travel, location, number of people traveling, number of travel days, and estimated cost.

The Travel Plan includes summary-level roll-ups by combined triplet SOW task, SOW Subtask, and Phase (e.g., Task 3, subtask 1, Phase 1); by month; and by the entire three-month period. Summary-level information includes: total number of trips, total number of people-trips (e.g., two people traveling on one trip is 2 people-trips), total number of days of travel, and total anticipated cost. Summary-level quantities for trips crossing month boundaries are prorated by the number of travel days occurring in the given month.

Contractor formatting of the Travel Plan is acceptable.

18.12 EOC Memorandum of Understanding

The MOU defines the roles and responsibilities of the ITOD's EOC in the performance of SENTINEL operations. The MOU shall define the expected EOC Help Desk Support. The contractor is responsible for all other operations and maintenance activities per the SOW. A sample MOU is appended below containing the expected EOC responsibilities.

Memorandum of Understanding

ITOD Support of SENTINEL Operation

To: (SENTINEL Program Manager) signature_____

From: Kenneth Boyd signature

Copy: Julius Brooks, Eileen Short, Helen Tracy, Janis Goldernik, John Taylor, Edward Sesak, Gale Scavenelli, James Tatum, Karen Jefferson, Rick Greenson

Date:

Re: ITOD's Enterprise Operations Center (EOC) support of SENTINEL operations

---

1. HelpDesk

The EOC's Customer Support (CS) staff will provide help desk assistance via the EOC's 202-324-1500 central support phone number for all problems and requests related to the SENTINEL system.

When the EOC CS staff receives a call from a customer requiring assistance, the CS staff will attempt to resolve the issue using the Call Scripts that were provided by the SENTINEL PMO.

If a user calls to request a SENTINEL password reset, the CS staff will resolve but all other account management requests (new, modified, delete account) will be assigned to the SENTINEL O&M contractor.

If a user calls regarding questions with SENTINEL the EOC CS staff will reference the caller to the SENTINEL website and log a ticket to the SENTINEL O&M contractor for resolution.

If the EOC CS staff cannot resolve the issue and the problems looks to be related to the SENTINEL software or hardware, the problem ticket will be assigned to the SENTINEL O&M contractor for resolution.

SENTINEL hours of Onsite Support: The SENTINEL staff will provide on-site support from 7:30 AM till 4:30 PM EST.

2. Network Service

The EOC's Network staff will not provide any monitoring or troubleshooting support to the SENTINEL network equipment.

3. System/Server Administration

The EOC's System/Server Administration staff will not provide any monitoring or troubleshooting support to the SENTINEL servers.

4. Security Management

The EOC's Security Management staff has no responsibilities for monitoring, account management, security logs, or remote patch management for SENTINEL. The EOC Security staff will provide the SENTINEL team the tested and approved McAfee virus updates via a compact disc.

5. Remote Software

The EOC's Remote Software staff has no responsibilities for software installation or Tier-2 troubleshooting.

6. Other Items to Address

SENTINEL Accounts Management is not a function of SARs and has not been transitioned to the Network Section's System Security Access Unit. All account requests will be facilitated via a problem ticket assigned to the SENTINEL assignment group.

SENTINEL Application support has not been transitioned to the Systems Support Section. All problems, upgrade and maintenance issues are the responsibility of the SENTINEL assignment group.

SENTINEL database support has not been transitioned to the Operation Section's Database Administration Unit. All problems, upgrade and maintenance issues related SENTINEL's databases are the responsibility of the SENTINEL assignment group.

The EOC will not provide 24 x 7 x 365 monitoring support of SENTINEL servers. The SENTINEL O&M contractor will be responsible for all monitoring, problems, upgrades and patch management.

The EOC will not provide 24 x 7 x 365 monitoring support of the SENTINEL network equipment. The SENTINEL O&M contractor will be responsible for all monitoring, problems, upgrades and patch management.

18.13 Risk Assessment (Delivered Twice Monthly)

The Risk Assessment is a report of the total risk exposure of each contractor-identified risk in accordance with the FBI Risk Management Guideline and Standards. The information reported for each active risk includes, at a minimum: unique identifier, title, short description, impact, probability of occurrence, timeframe of concern, and changes in impact, probability of occurrence, and timeframes of concern relative to the preceding report. Tables within the Risk Assessment provide different views of the information by sorting on different elements of information. Specific tables of active risks to be included are:

a. Sort by risk identifier (all active risks in order of increasing identifier)
b. Sort by impact (top *N* active risks in order of decreasing identifier)
c. Sort by probability of occurrence (top *N* active risks in decreasing order of probability)
d. Sort by timeframe (*N* earliest active risks in order of increasing start date)
e. Sort by change in impact (*N* largest changes in decreasing order)
f. Sort by change in probability (*N* largest changes in decreasing order)
g. Sort by change in timeframe (*N* earliest risks whose start dates shift from prior report)

At contract initialization, the value *N* will be specified for each table, although its value may change during the course of the contract to satisfy government needs. The Risk Assessment also summarizes the risks that were closed relative to the preceding report.

Contractor formatting of the Risk Assessment is permitted.

18.14 Integrated Master Schedule (weekly)

Integrated Master Schedule (IMS)	Item Number: B-2-14
	Revision #: R01
	Effective Date: 05-28-04

Use

The Integrated Master Schedule (IMS) is an integrated schedule containing the networked, detailed tasks necessary to ensure successful program execution. The IMS shall be used to verify attainability of contract objectives, to evaluate progress toward meeting program objectives, and to integrate the program schedule activities with all related components. The IMS includes significant external interfaces and critical items from suppliers, teammates, or other detailed schedules that depict significant and/or critical elements and Government furnished equipment or information dependencies for the entire contractual effort in a single integrated network.

Interrelationship

The IMS is traceable to the Project Plan, the Work Breakdown Structure (WBS), the Earned Value Management System (EVMS) Baseline and the Statement of Work (SOW). The written document and the associated electronic deliverable are delivered to the Project Manager and the Contracting Officer (if the project is part of a contract)

Preparation information

Preparation of the written IMS Analysis

The IMS Analysis is an assessment of schedule progress to date and includes changes to schedule assumptions, variances to the baseline schedule, causes for the variances, potential impacts, and recommended corrective actions to minimize schedule delays. The analysis shall also identify potential problems and an assessment of the critical path and near-critical paths. The thresholds for reporting significant variances to the baseline schedule are any differences between current schedule date and baseline schedule date for milestones (zero duration) or plus or minus 10% of duration for other tasks/activities. The near critical path is defined as any task/activity with a total float/slack of five work days or less.

Preparation of the Electronic IMS Data Report

1.0 Format

The electronic IMS data shall be reported using Microsoft Project 2003. The electronic IMS data shall be delivered electronically in a Microsoft Project 2003 format, specifically a single *.mpp file or a master *.mpp file accompanied by the linked subproject files in a *.mpp file format.

2.0 Content

The schedule shall contain the contract milestones, accomplishments, and discrete tasks/activities (including planning packages where applicable) from contract award to the completion of the contract. The schedule shall be an integrated, logical network-based schedule that correlates to the WBS, and is vertically and horizontally traceable to the cost/schedule reporting instruments used to address variances such as the EVMS Status Report. It shall contain contractual milestones and descriptions and display summary, intermediate, and detailed schedules, and periodic

analysis of progress to date. It shall include fields and data that enable the user to access the information by product, process, or organizational lines.

2.1 Contract Milestones and Definitions

The schedule shall contain key programmatic events, which define progress and completion for each WBS element, along with the definition for successful completion of the milestone.

2.2 Summary Master Schedule

This schedule shall contain a top-level schedule of key tasks/activities and milestones at the summary levels of the WBS. It shall be an integrated roll up of the intermediate and detailed schedules (see 2.3 and 2.4 below) (vertical integration).

2.3 Intermediate Schedules

These schedules shall be mid-level contract schedules that include key tasks/activities and milestones and all associated accomplishments in the summary master schedule, traceable to the WBS element to display work effort at the intermediate level of summarization. There may be several intermediate schedules that depict varying levels of detail. They shall be integrated roll ups of the detailed schedules (see 2.4 below) (vertical integration).

2.4 Detailed Schedules

These schedules are the lowest level of contract tasks/activities that form the network. The detailed schedules shall contain horizontal and vertical integration, as a minimum, at the work package and planning package level. The detailed schedules shall include all tasks/activities, work packages, and planning packages identified resulting from the Statement of Work (SOW). Every discrete task/activity, work package, and planning package shall be clearly identified and directly related to a control account. Work packages and planning packages shall be individually represented and summarize to or reconcile with the total budget for that control account. If Level of Effort (LOE) control accounts, work packages, or planning packages are included as tasks in the IMS, they shall be clearly identified as such. The detailed tasks/activities, work packages, and planning packages shall be traceable to only one WBS element and only one responsible/performing organizational element, as applicable. The level of detail in the IMS (including number and duration of tasks/activities) shall follow the contractor's EVM process as documented in the EVMS system description, EVMS Baseline program directives, etc. Shorter-term work packages (ideally equal in length to the statusing interval) are preferred because they provide more accurate and reliable measures of work accomplished.

2.4.1 Key Elements of Detailed Schedules

The key elements of the detailed schedules include the following:

1) Task/Activity - An element of work with duration.

2) Milestone - A specific definable accomplishment in the contract network, recognizable at a particular point in time. Milestones have zero duration and do not consume resources.

3) Duration - The length of time estimated (or realized) to accomplish a task/activity.

4) Percent Complete (Schedule) - The proportion of an activity or task that has been completed to time now. This usually involves updating or statusing the activity or task utilizing one of two methods: (1) Update the remaining time to complete (remaining duration) and the scheduling software will then automatically update the schedule percent complete or (2) update the schedule percent complete and allow the scheduling software to calculate the time remaining (remaining duration) to complete. Either method will use the following formula: Percent of Duration Completed = (Actual Duration / Total Duration) X 100.

5) Task/Activity and Milestone Descriptions - These are descriptive titles that are concise, complete, and clearly identify the work effort being accomplished. Abbreviations may be used to shorten the descriptive titles.

6) WBS Codes and Data Dictionary - A list of field definitions and WBS structures. This list shall be provided to the procuring activity.

7) Relationship/Dependency - These identify how predecessor and successor tasks/activities and milestones are logically linked. Relationships, also called network logic, are modeled in four ways:

a) FS (Finish to Start) - A predecessor task/activity or milestone that must finish before a succeeding task/activity or milestone can start. FS relationships shall be used whenever possible.

b) SS (Start to Start) - A predecessor task/activity or milestone that must start before a succeeding task/activity or milestone can start.

c) FF (Finish to Finish) - A predecessor task/activity or milestone that must finish before a succeeding task/activity or milestone can finish.

d) SF (Start to Finish) - A predecessor task/activity or milestone that must start before a succeeding task/activity or milestone can finish.

8) Total Float/Slack - The amount of time a task/activity or milestone can slip before it delays the contract or project finish date.

9) Free Float/Slack - The amount of time a task/activity or milestone can slip before it delays any of its successor tasks/activities or milestones.

10) Lag - An interval of time that must occur between a predecessor and successor task/activity or milestone. Since negative time is not demonstrable, negative lag is not encouraged. (Note: Lag should not be nsed to manipulate float/slack or constrain schedule.)

11) Early Start (ES) - The earliest start date a task/activity or milestone can begin the precedence relationships. A computer-calculated date.

12) Early Finish (EF) - The earliest finish date a task/activity or milestone can end. A computer-calculated date.

13) Late Start (LS) - The latest start date a task/activity or milestone can start without delaying the contract or project target completion date. A computer-calculated date.

14) Late Finish (LF) - The latest date a task/activity or milestone can finish without delaying the contract or project target completion date. A computer-calculated date.

15) Critical Path - A sequence of discrete tasks/activities in the network that has the longest total duration through the contract or project. Discrete tasks/activities along the critical path have the

least amount of float/slack. The critical path and near-critical paths are calculated by the scheduling software application. The guidelines for critical path and near-critical path reporting are as follows:

a) Methodology - The IMS software application computes a critical path and near-critical paths based on precedence relationships, lag times, durations, constraints, and status. Artificial constraints and incorrect, incomplete, or overly constrained logic shall be avoided because they can skew the critical path and near-critical paths.

b) Identification - The critical path shall be easily identified.

16) Constraints - Limits applied to network start and finish dates (e.g., "finish no later than"). (Note: Certain types of constraints should be used judiciously because they may impact or distort the network critical path.)

17) Current Schedule - The IMS reflects the current status and forecast. It includes forecasted starts and finishes for all remaining tasks/activities and milestones. Significant variances to the baseline schedule shall be explained in the periodic analysis. Thresholds for reporting shall be specified in the Data Items.

18) Baseline Schedule - Baseline dates in the IMS shall be consistent with the baseline dates in the EVMS Baseline for all work packages, planning packages, and control accounts (if applicable). The guidelines for maintaining the baseline schedule are as follows:

a) Schedule Changes - Changes to the schedule shall be baselined when incorporated into the schedule.

b) Baseline Schedule Changes - Changes to the baseline schedule shall be made in accordance with the Contracting Officer approved EVM process. Any movement of contractual milestones in the baseline schedule shall be derived only from either authorized contract changes or an approved over target schedule.

19) Schedule Progress - The IMS shall reflect actual progress and maintain accurate start and finish dates for all tasks/activities and milestones. The guidelines for reflecting schedule progress are as follows:

a) Actual Start and Finish Dates - Actual start and actual finish dates shall be recorded in the IMS. Actual start and actual finish dates, as recorded, shall not be later than the status date.

b) Progress Line - The progress line depicted in a Gantt chart shall be applied to the current schedule.

20) Retention of Data for Completed Tasks/Activities -Historical performance on completed tasks/activities shall be maintained electronically for analytical use. Historical performance shall be maintained at the time of key program events (Integrated Baseline Review, Critical Design Review, etc.) for all critical tasks/activities. Data to be retained includes logic, actual and baseline durations, actual and baseline start and finish dates, and the three-point estimates that were used before the task/activity started.

21) External Dependencies - The IMS shall identify significant external dependencies that involve a relationship or interface with external organizations, including all Government furnished items (e.g., decisions, facilities, equipment, information, data, etc.). The determination of significant shall be agreed to by the Government and contractor and shall be defined and documented in the Data Items. The required or expected delivery dates shall also be identified in the IMS.

22) Schedule Margin - A management method for accommodating schedule contingencies. It is a designated buffer and shall be identified separately and considered part of the baseline. Schedule

margin is the difference between contractual milestone date(s) and the contractor's planned date(s) of accomplishment.

23) Schedule Risk Assessment - A schedule risk assessment predicts the probability of project completion by contractual dates. Three-point estimates shall be developed for remaining durations of remaining tasks/activities that meet any of the following criteria: (1) critical path tasks/activities, (2) near-critical path tasks/activities (as specified above), and (3) high risk tasks/activities in the program's risk management plan. These estimates include the most likely, best case, and worst case durations. They are used by the contractor to perform a probability analysis of key contract completion dates. The criteria for estimated best and worst case durations shall be applied consistently across the entire schedule and documented in the contractor's sehedule notes and management plans. The guidelines for estimates are as follows:

a) Most Likely Estimate - Schedule durations based on the most likely Estimates.

b) Best/Worst Case Estimates - Best and worst case assumptions shall be disclosed.

The contractor schedule risk assessment shall explain changes to the critical path, margin erosion, and mitigation plans. It shall be incorporated into the contractor's program risk management process. The initial schedule risk assessment shall be submitted during the Integrated Baseline Review. The risk analysis may be performed within the IMS or within a separate risk tool as appropriate based on the capability of the automated scheduling tool.

24) User Defined Fields - All user defined fields in the IMS shall be identified by providing a mapping of all fields used in the scheduling software application.

25) Reserved Fields - The Government may reserve some fields and/or require the contractor to use certain fields for specific information.

Calendar - The arrangement of normal working days, together with non-working days, such as holidays, as well as special work days (i.e., overtime periods) used to determine dates on which project work will be completed.

18.18 Data Accession List

The contractor shall maintain a current listing of all Program Documentation including title, version, date and location.

18.25 Design Concept Description and Architecture

Use the FBI IT LCMD Appendix H Design Concept Description with the following addition as an appendix to address the Security Architecture as follows:

Appendix A – SENTINEL Security Architecture

1. OVERVIEW AND REQUIREMENTS
1.1 SENTINEL System Architecture Overview
1.2 Security Requirements and Policies
1.3 Philosophy of Protection
1.4 C&A Strategy
1.4.1 Availability
1.4.2 Confidentiality
1.4.3 Data Integrity
1.5 Assumptions and Constraints
2. SENTINEL SYSTEM SECURITY ARCHITECTURE APPROACH
2.1 SENTINEL Security Functions
2.1.1 Identification and Authentication (I&A)
2.1.2 User Authorization
2.1.3 User Account Administration
2.1.4 Filtering and Anomaly Detection
2.1.5 Access Control
2.1.6 Auditing and Audit Reporting
2.2 SENTINEL Security Implementation
2.2.1 Security Server
2.2.2 Directory Server
2.2.3 Discretionary Access Controls
2.3 Data Integrity
2.4 Security Organizational Controls
2.4.1 System Administrator (SYSADMIN)
2.4.2 Configuration Management Manager (CMM)
2.4.3 Information Systems Security Manager (ISSM)
2.4.4 Computer System Security Officer (CSSO)
2.5 Legacy Interfaces
2.6 Communications Networks
2.7 Physical Security

18.36 Service Level Agreement (SLA)

The SLA shall be developed in a Government approved contractor specified format. The SLA shall contain the following elements:

Duration - Specify when the agreement begins and expires.

Roles and responsibilities-Define the roles and responsibilities of the customer, the Government service level manager, and the service provider.

Descriptions of service- Include specific descriptions of the services to be provided (a service catalog), including applications, infrastructure, and other business functions.

Service standards – Define the performance targets to be met. Reference sources where available (e.g., SOW, SRS). Define operating hours for each service and associated levels of service.

Sample Measurements and Performance Targets

Measurement	Definition	Performance Target
SLA Table from SOW Section 15		
SENTINEL system availability		Per the SRS
SENTINEL system response time		Per the SRS
SENTINEL capacity management		Per the SRS
SENTINEL data backup		Per the SRS, PUG
SENTINEL personnel response time		1 hour
SENTINEL periodic maintenance time		Not to exceed two hours per week
SENTINEL disaster recovery times		Per the contingency plan
SENTINEL user account set up time		
Trouble ticket response times		Per the EOC handbook
Trouble ticket resolution times		Per the EOC handbook
Alert deadlines (low medium, high, critical)		Per the EOC handbook

Evaluation Methods and Reports -Establish objective means to determine how well the system and the O&M team are delivering to the service standards. Establish the reports, source of data and frequency of reporting.

Policies, Procedures, Standards – Reference the policies, procedures, and standards to be employed in support of the services covered under this SLA.

Incentives and Penalties- Establish the incentives with achieving or exceeding target levels. Establish penalties associated with not meeting targets.

18.39 Data Migration Plan

Identify the scope of the data migration efforts (e.g., what data elements to be migrated, whether open transactional data will migrate, the amount of historical data to convert, error correction plan). Describe the data migration process, to include the roles and responsibilities of participants and the identity of the process owner. Identify potential risks, verification strategies, migration dependencies, and volume considerations. Provide specific and measurable criteria for migration success. Provide a data migration schedule, by Phase, that includes when the data will be captured, converted, verified for correctness and completeness, and available for use in the new system software.

By project Phase, identify for each file of migrating data:

- Location of migrating data
- Legacy software that accessed migrating data
- Quantity of migrated data
- Form of data
- Conversions required to be compatible with new system
- Error correction requirements
- New software that will access the migrated data
- Expected size of migrated data
- Expected location of migrated data
- Means of verifying correctness and completeness of data migration

The contractor formatting of the Data Migration Plan is acceptable.

18.40 EOC Operational Support Requirements Document of New Systems

Federal Bureau of Investigation
Information Resources Division
Customer Relations Management Section
Enterprise Operations Center Unit

EOC OPERATIONAL SUPPORT REQUIREMENTS DOCUMENT FOR NEW SYSTEMS

Program/System Name:
Brief Description of System:

FBI Program Manager: **Phone:**
Security/C&A POC: **Phone:**
ISSM: **Phone:**
ISSO: **Phone:**
Sponsor: **Phone:**
Technical Lead: **Phone:**
Pager:

Operational Support Plan

- **Implementation schedule**

_____

_____

_____

- **Division/Section/Unit(s)** that provides Tier2 Support (Touch Labor)

  _____

  Hours Supported:

  _____

- **Division/Section/Unit(s)** that provides Tier3 Support (Application and/or Engineering)

  _____

  Hours Supported:

  _____

- **Division/Section/Unit(s)** that provides Access Support

  _____

  Hours Supported:

  _____

EOC Standard Operating Procedures (Attach Docs)

- **Call Scripts**: Yes / No
- **Frequently Asked Questions & Answers**: Yes / No

EOC Transition Plan

- **For EOC Tier 1 HelpDesk**
- **For EOC Tier 1 System Administration**
- **For EOC Tier 1 Network Services**
- **For EOC Tier 1 Security Management**

Additional EOC Support Resources:

- **Costs Associated with Resources**
  $ _____

EOC Training

- **For EOC Tier 1 HelpDesk**
- **For IRD Tier 1 System Administration**
- **For EOC Tier 1 Network Services**
- **For EOC Tier 1 Security Management**

Hardware Associated with new System?

- Yes / No
- If yes, explain and complete below.

Property Number	Serial No	Device Type	CostCode

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00203 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.144

EOC Server/Mainframe Monitoring Required?

- Yes / No
- If yes, explain.

- EMS Tools Used

- New EMS Tools Needed
  Yes / No
  If yes, explain.

Software Associated with new System?

- Yes / No
- If yes, list software below

Software Name	Platform (e.g. Mainframe, Server, Desktop)

Database Associated with new System?

- Yes / No
- If yes, list software below

Database Name	Platform (e.g. Mainframe, Server, Desktop)

Operational Level Agreements (OLA's)

(Response times between EOC and IRD/Contract Support Staff)

Service Level Agreements (SLA's)

(Providing resolution times to the customer by Subcategory)

Critical Page List

Last, First, MI	Pager	Position

Additional EOC Support Costs

- **Resources**
  $ _____
- **Software**
  $ _____
- **Hardware**
  $ _____

- **Categories/Subcategories/Assignment Groups**

CATEGORY - SUBCATEGORY - DIV/SECTION/UNIT - DESCRIPTION

Application_____
Application_____
Application_____
Application_____
Software_____
Software_____
Software_____
Software_____
Hardware_____
Hardware_____
Hardware_____
Hardware_____
Network_____
Network_____
Network_____
Network_____
Security_____
Security_____
Security_____
Security_____
User_____
User_____
User_____
User_____

ServiceCenter Access Needed?

Yes / No

ServiceCenter Access Procedures.

Each person that requires access to ServiceCenter will require a SAR (http://itod.fbinet.fbi/sc/sar/sarhqdivisionpoc.pdf) to be opened for FBINet Mainframe access first (http://itod.fbinet.fbi/sc/scaccess.htm). The process is below.

To Request:

- New or modified access to one (or many) of the ServiceCenter Application's modules ...
- Removal of access to the ServiceCenter Application ...
- Accessor ID (ACID) login changes to the ServiceCenter Application ...
- Email address changes to the ServiceCenter application.

You Must Have:

- FBINET accessor ID issued by Systems Security Access Unit . If you do not have an ACID, a SAR will need to be submitted.(http://itod.fbinet.fbi/sc/sar/sarhqdivisionpoc.pdf)
- A current record in the BPMS system. (If non-FBI with an FBINET ACID, enter a record via PCUS. (http://30.100.100.8:8180/contact/servlet/Contact)

Follow these steps:

1. Fill out and print the ServiceCenter Access Request Form. If you select OTHER as the "user's job type" on the basic access request form, also complete the Amended ServiceCenter Access Request Form.
2. Complete the mandatory fields and the specific type of access you are requesting.
3. Have your supervisor sign the form to validate request.
4. Fax completed form(s) to (202) 324-6720, Attention: IIAU-SCPT.

A Service Problem ticket will be opened and assigned to D4/SDS/IISCU-SCPT for processing. A member of the ServiceCenter Program Team (SCPT) will notify the requester once the access has been granted.

ISSUES/CONCERNS/COMMENTS

18.41 DCU04 Request for Data Center Access

DCU04 Rev. 11/14/04

Request For Data Center Access

Program Name: _____ Date:

Program Manager: _____ Room:

Division / Section / Unit: _____ Ext: _____

Name	Company / Agency	Clearance Level	Access Begin Date	Access End Date	Access Type	Escort Authority (Yes/No)

(Note: When bringing equipment into the Data Center, a completed DCU05 form "Data Center Equipment Installation Requirements" is required before the equipment may enter Data Center space.)

Instructions

Name: Name of person(s) needing access
Company/Agency: Employing company/agency
Clearance Level: Clearance granted by FBI - include SCI access if applicable
Access Begin Date: Requested date to begin access to the Data Center
Access End Date: Date to end access to the Data Center (note: access must be updated semi-annually)
Access Type: Unrestricted (Only FBI Personnel Assigned In Data Center), Unescorted (must have TS/SCI), or Escorted
Escort Authority: Request to allow this person to escort (must be an FBI employee with TS/SCI)

_____
(Requesting Unit Chief) Date

_____
(DCU Chief) Date

18.42 DCU05 Request for Data Center Equipment Installation

DCU05 11/03

REQUEST FOR DATA CENTER EQUIPMENT INSTALLATION

Program Name: _____ Date: _____

Program Manager: _____ Room: _____

Division / Section / Unit: _____ Ext. _____

DESCRIPTION OF EQUIPMENT TO BE INSTALLED AND SPACE/POWER COOLING/CONNECTIVITY REQUIRED:

Examples:

(2105) Server	1 5	13-23-65/F1111111 2R85V21/F1323900	IBM(Z900) via Ficon FBINET via Gigabit Ethernet	L6-30R(2) Nema 5-15(6)	60 15	DUAL DUAL Or SINGLE	47 KBTU 2400 BTU	5"x9" 4"x12"

Item Make/Model	Qty	Serial# and Property#	Connects to: attach wiring diagram	Power Recept Type/#	Power Amps	UPS Connect	Hea BTU

Notes: Attach equipment diagram with physical size and space needed to service equipment.

_____
(Requesting Unit Chief) Date

_____
(DCU Chief) Date

18.53 Technical Manual (Non-Commercial HW only)

Use the guidelines established in FBI IT LCMD Appendix H with the following additional guidance: Commercial manuals shall be delivered and are considered suitable substitutes for the technical manual. Technical manuals are only required in the event a commercial manual is not available, modifications are made to off the shelf hardware, or custom hardware is developed.

18.65 Product (CSCI's)

This is the physical software.

18.66 Logical Data Model

The contractor shall develop a logical data model using the Government model as point of departure. The content shall include, at a minimum, the same type of information contained in the Government model. The data model shall be exportable to the Government data modeling tool (ERWIN).

18.68 O&M Procedures

The contractor shall prepare supplemental procedures to assist the TIER 1 Call Center, operations, etc., as required to support, streamline and enhance operations and maintenance. Contractor format is acceptable.

18.69 O&M Transition Plan

1. Scope. This section shall be divided into the following paragraphs.

1.1 Identification. This paragraph shall contain a full identification of the system to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).

1.2 System Overview. This paragraph shall briefly state the purpose of the system to which this document applies. It shall describe the general nature of the system; and summarize operation and maintenance activities; and list other relevant documents.

1.3 Document Overview. This paragraph shall summarize the purpose and contents of this document and shall describe any security or privacy considerations associated with its use.

2. Referenced Documents. This section shall list the number, title, revision, and date of all documents referenced in this report. This section shall also identify the source for all documents not available through normal Government stocking activities.

3. Transition Plan. This section shall be divided into the following paragraphs to provide an overview of the Transition Plan. To include all activities, facilities, documentation, Government assistance, and incumbent contractor assistance needed to successfully transition from the current operations and maintenance support contract to the operations and maintenance contract resulting from this solicitation.

3.1 Overall process to accomplish Transition Plan objectives. This paragraph(s) shall, at a minimum, address the following:

a. Introduction: Introduces this Transition Plan and discusses the scope, objective, and summary of the transition process.

b. Documentation: Lists the Transition Plan guidance documents and information documents. Presents a documentation tree for the documents needed to implement the transition process.

c. Transition Overview: Presents an executive overview of the transition process and provides a Transition Overview Diagram for easy reference.

d. Transition Management: Describes the method for managing the transition process. Describes the method and measures for measuring the transition process success.

e. Transition Resources: Describes the resources needed to implement the transition process. Describes roles and responsibilities in completing the transition process.

f. Transition Tasks: Describes the tasks to be accomplished to complete the transition process. Included in the tasks shall be the activities needed to seamlessly integrate contracted services into the CJIS System-of-Services.

g. Task Dependencies: Describes the task dependencies and establishes a master schedule.

h. Assumptions and Constraints: Describes assumptions and constraints used within the transition process.

i Transition Cost Estimate, Not-to-Exceed Transition Price, and basis for those estimates.

3.2 Recommended Improvements. This paragraph shall provide any recommended improvements in the operation and maintenance activities that support transition. A discussion of each recommendation and its impact on the system may be provided. If no recommended improvements are provided, this paragraph shall state "None."

4. Notes. This section shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

18.70 SENTINEL Stakeholder and Organizational Risk Assessment

A template for the SENTINEL Stakeholder and Organizational Risk Assessment is provided at SOW Attachment-7 Communications and Strategy Action Plan template. SOW Attachment-7 contains the Government's desired plan content and level of detail. The plan shall address the topics contained in the attachment.

18.71 Organization Impact Assessment (OIA)

A template for the Organizational Impact Assessment is provided at SOW Attachment-8 Organizational Impact Assessment template. SOW Attachment-8 contains the Government's desired plan content and level of detail. The plan shall address the topics contained in the attachment.

18.76 Agendas, Briefings, Meeting Minutes

Content shall be at the contractor's discretion and judgment to meet the purpose of the supported conference/meeting/review.

18.77 Workforce Transformation Strategy and Plan

A template for the Workforce Transformation Strategy and Plan is provided at SOW Attachment-9 Workforce Transformation Strategy and Plan template. SOW Attachment-9 contains the Government's desired plan content and level of detail. The plan shall address the topics contained in the attachment.

18.78 Integrated Master Plan

The Integrated Master Plan shall conform to the IMP content guidelines contained in AFMC Pamphlet 63-5, Integrated Master Plan and Schedule Guide 11 November 2004. The IMP shall include key process descriptions.

18.79 Training Strategy and Plan

A template for the Training Strategy and Plan is provided at SOW Attachment-6 Training Strategy and Plan template. SOW Attachment-6 contains the Government's desired plan content and level of detail. The plan shall address the topics contained in the attachment.

18.80 Training Administration Report

A template for a Training Administration Report is provided at SOW Attachment-10 Training Administration Report template. The attachment contains the Government desired report content. The report shall address the topics contained in the attachment.

18.81 Delivery Acceptance Report

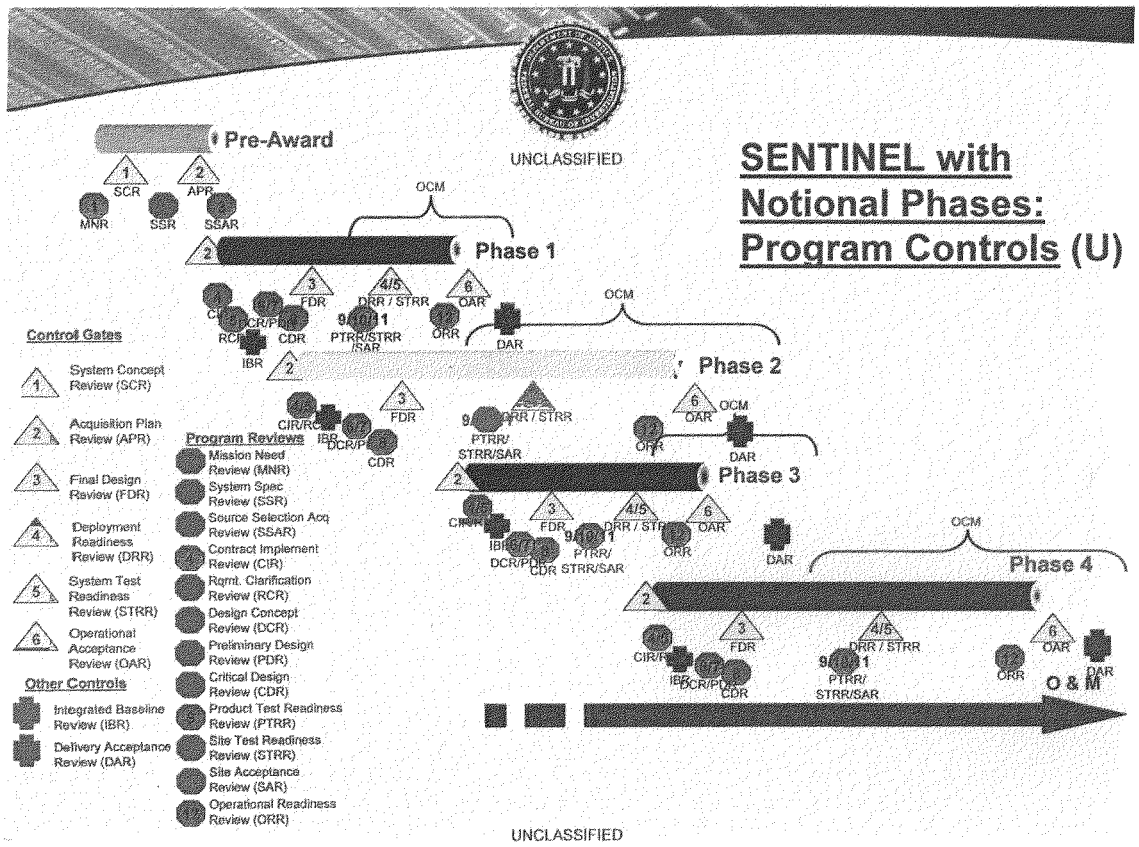
TBS Offeror to propose.

ENCLOSURE B

QUESTION 11d

SENTINEL MILESTONES

46051.155


SENTINEL with Notional Phases: Program Controls (U)
UNCLASSIFIED
Pre-Award
Phase 1
Phase 2
Phase 3
Phase 4
O & M
OCM
SCR
APR
MNR
SSR
SSAR
FDR
DRR / STRR
OAR
CDR
ORR
DAR
IBR
PTRR/STRR /SAR
PTRR/ STRR/SAR
Control Gates
System Concept Review (SCR)
Acquisition Plan Review (APR)
Final Design Review (FDR)
Deployment Readiness Review (DRR)
System Test Readiness Review (STRR)
Operational Acceptance Review (OAR)
Other Controls
Integrated Baseline Review (IBR)
Delivery Acceptance Review (DAR)
Program Reviews
Mission Need Review (MNR)
System Spec Review (SSR)
Source Selection Acq Review (SSAR)
Contract Implement Review (CIR)
Rqmt. Clarification Review (RCR)
Design Concept Review (DCR)
Preliminary Design Review (PDR)
Critical Design Review (CDR)
Product Test Readiness Review (PTRR)
Site Test Readiness Review (STRR)
Site Acceptance Review (SAR)
Operational Readiness Review (ORR)
UNCLASSIFIED

ENCLOSURE C

QUESTION 22b

NATIONAL RESPONSE PLAN

1. **Terrorism Incident Law Enforcement and Investigation Annex**

2. **Nuclear/Radiological Incident Annex**

3. **Biological Incident Annex**

46051.157

ENCLOSURE C

1. Terrorism Incident Law Enforcement and Investigation Annex

46051.158

Terrorism Incident Law Enforcement and Investigation Annex

Coordinating Agency:

Department of Justice/Federal Bureau of Investigation

Cooperating Agencies:

Department of Defense
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of State
Environmental Protection Agency

Introduction

Purpose

The purpose of this annex is to facilitate an effective Federal law enforcement and investigative response to all threats or acts of terrorism within the United States, regardless of whether they are deemed credible and/or whether they escalate to an Incident of National Significance. To accomplish this, the annex establishes a structure for a systematic, coordinated, unified, timely, and effective national law enforcement and investigative response to threats or acts of terrorism within the United States.

Scope

This annex is a strategic document that:

- Provides planning guidance and outlines operational concepts for the Federal law enforcement and investigative response to a threatened or actual terrorist incident within the United States; and
- Acknowledges and outlines the unique nature of each threat or incident, the capabilities and responsibilities of the local jurisdictions, and the law enforcement and investigative activities necessary to prevent or mitigate a specific threat or incident.

Policies

The United States regards terrorism as a potential threat to national security, as well as a violent criminal act, and applies all appropriate means to combat this danger. In doing so, the United States vigorously pursues efforts to deter and preempt these crimes and to apprehend and prosecute directly, or assist other governments in prosecuting, individuals who perpetrate or plan terrorist attacks.

To ensure the policies established in applicable Presidential directives are implemented in a coordinated manner, this annex provides overall guidance to Federal, State, local, and tribal agencies concerning the Federal Government's law enforcement and investigative response to potential or actual terrorist threats or incidents that occur in the United States, particularly those involving weapons of mass destruction (WMD), or chemical, biological, radiological, nuclear, or high-explosive (CBRNE) material.

Federal Agencies

The law enforcement and investigative response to a terrorist threat or incident within the United States is a highly coordinated, multiagency State, local, tribal, and Federal responsibility. In support of this mission, the following Federal agencies have primary responsibility for certain aspects of the overall law enforcement and investigative response:

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00218 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.159

- Department of Defense (DOD)
- Department of Energy (DOE)
- Department of Health and Human Services (HHS)
- Department of Homeland Security (DHS)
- Department of Justice/Federal Bureau of Investigation (FBI)
- Environmental Protection Agency (EPA)

According to HSPD-5, "The Attorney General has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at U.S. citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States, as well as for related intelligence collection activities within the United States, subject to the National Security Act of 1947 and other applicable law, Executive Order 12333, and Attorney General-approved procedures pursuant to that Executive order. Generally acting through the Federal Bureau of Investigation, the Attorney General, in cooperation with other Federal departments and agencies engaged in activities to protect our national security, shall also coordinate the activities of the other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States. Following a terrorist threat or an actual incident that falls within the criminal jurisdiction of the United States, the full capabilities of the United States shall be dedicated, consistent with U.S. law and with activities of other Federal departments and agencies to protect our national security, to assisting the Attorney General to identify the perpetrators and bring them to justice. The Attorney General and the Secretary shall establish appropriate relationships and mechanisms for cooperation and coordination between their two departments."

Although not formally designated under this annex, other Federal departments and agencies may have authorities, resources, capabilities, or expertise required to support terrorism-related law enforcement and investigation operations. Agencies may be requested to participate in Federal planning and response operations, and may be requested to designate liaison officers and provide other support as required.

Deployment/Employment Priorities

In addition to the priorities identified in the National Response Plan (NRP) Base Plan, the law enforcement and investigative response to terrorist threats or incidents is based on the following priorities:

- Preserving life or minimizing risk to health; which constitutes the first priority of operations.
- Preventing a threatened act from being carried out or an existing terrorist act from being expanded or aggravated.
- Locating, accessing, rendering safe, controlling, containing, recovering, or disposing of a WMD that has not yet functioned, and disposing of CBRNE material in coordination with appropriate departments and agencies (e.g., DOD, DOE, EPA).
- Apprehending and successfully prosecuting perpetrators of terrorist threats or incidents.

Planning Assumptions and Considerations

In addition to the planning assumptions and considerations identified in the NRP Base Plan, the law enforcement and investigative response to terrorist threats or incidents, particularly those involving WMD and CBRNE material, are based on the following assumptions and considerations:

- A terrorist threat or incident may occur at any time of day with little or no warning, may involve single or multiple geographic areas, and may result in mass casualties.
- The suspected or actual involvement of terrorists adds a complicating dimension to incident management.
- The response to a threat or actual incident involves FBI law enforcement and investigative activity as an integrated element.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00219 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.160

- In the case of a threat, there may be no incident site, and no external consequences, and, therefore, there may be no need for establishment of traditional Incident Command System (ICS) elements such as an Incident Command Post (ICP) or a Joint Field Office (JFO).
- An act of terrorism, particularly an act directed against a large population center within the United States involving nuclear, radiological, biological, or chemical materials, will have major consequences that can overwhelm the capabilities of many local, State, and/or tribal governments to respond and may seriously challenge existing Federal response capabilities.
- In the case of a biological attack, the effect may be temporally and geographically dispersed, with no determined or defined "incident site." Response operations may be conducted over a multijurisdictional, multistate region.
- A biological attack employing a contagious agent may require quarantine by Federal, State, local, and tribal health officials to contain the disease outbreak.
- If appropriate personal protective equipment and capabilities are not available and the area is contaminated with CBRNE or other hazardous materials, it is possible that response actions into a contaminated area may be delayed until the material has dissipated to a level that is safe for emergency response personnel to operate or until appropriate personal protective equipment and capabilities arrive, whichever is sooner.

Situation

The complexity, scope, and potential consequences of a terrorist threat or incident require that there be a rapid and decisive capability to resolve the situation. The resolution to an act of terrorism demands an extraordinary level of coordination of law enforcement, criminal investigation, protective activities, emergency management functions, and technical expertise across all levels of government. The incident may affect a single location or multiple locations, each of which may be an incident scene, a hazardous scene, and/or a crime scene simultaneously.

Concept of Operations

Command and Control

The FBI is the lead agency for criminal investigations of terrorist acts or terrorist threats and intelligence collection activities within the United States. Investigative and intelligence activities are managed by the FBI from an FBI command post or Joint Operations Center (JOC). The command post or JOC coordinates the necessary Federal law enforcement assets required to respond to and resolve the threat or incident with State, local, and tribal law enforcement agencies.

The FBI Special Agent in Charge (SAC) of the local Field Office establishes a command post to manage the threat based upon a graduated and flexible response. This command post structure generally consists of three functional groups: Command, Operations, and Operations Support, and is designed to accommodate participation of other agencies, as appropriate (see Figure 1).

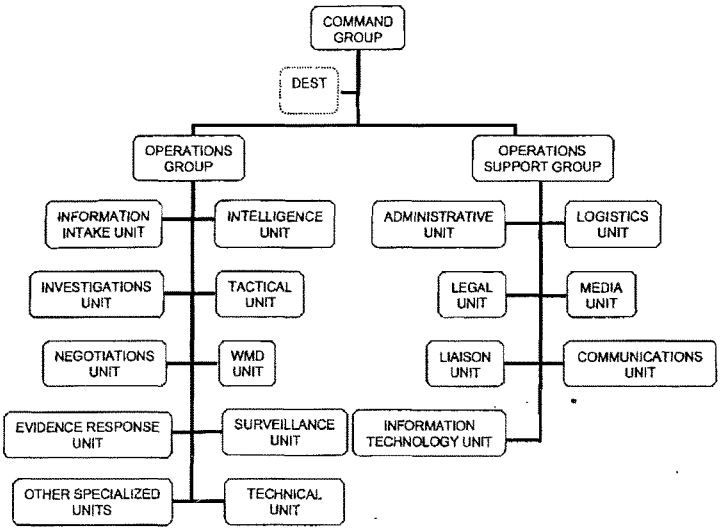
When the threat or incident exceeds the capabilities and resources of the local FBI Field Office, the SAC can request additional assistance from regional and national assets to augment existing capabilities. In a terrorist threat or incident that may involve a WMD or CBRNE material, the traditional FBI command post will transition to a JOC, which may temporarily incorporate a fourth functional entity, the Consequence Management Group (see Figure 2), in the absence of an activated JFO.

When, in the determination of the Secretary of Homeland Security, in coordination with the Attorney General, the incident becomes an Incident of National Significance and a JFO is established, the JOC becomes a section of the JFO and the FBI SAC becomes the Senior Federal Law Enforcement Official (SFLEO) in the JFO Coordination Group. In this situation, the JOC Consequence Management Group is incorporated into the appropriate components of the JFO (see NRP Base Plan, Figure 4 and Figure 7).

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00220 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.161

FIGURE 1. FBI command post



VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00221 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.162

The JOC structure may also be used to coordinate law enforcement, investigative, and intelligence activities for the numerous threats or incidents that occur each year that do not escalate to Incidents of National Significance.

Joint Operations Center

- The JOC is an interagency command and control center for managing multiagency preparation for, and the law enforcement and investigative response to, a credible terrorist threat or incident. Similar to the Area Command concept within the ICS, the JOC also may be established to coordinate and organize multiple agencies and jurisdictions during critical incidents or special events. Following the basic principles established in the National Incident Management System (NIMS), the JOC is modular and scalable and may be tailored to meet the specific operational requirements needed to manage the threat, incident, or special event.

- A JOC may be established and staffed in a pre-incident, pre-emptive role in support of a significant special event. This "watch mode" allows for rapid expansion to full operations if a critical incident occurs during the special event. The JOC is a strategic management tool that effectively coordinates law enforcement investigative, intelligence, and operational activities at multiple sites from a single location. The JOC may be the only management structure related to a threat, critical incident, or special event, or it may integrate into other management structures in accordance with the NRP.

- Law enforcement public safety functions, such as proactive patrol and traffic control, historically are managed through the Operations Section of the ICS. Criminal investigation and the collection, analysis, and dissemination of intelligence are sensitive law enforcement operations that require a secure environment and well-defined organizational management structure. The JOC is designed to coordinate this specialized law enforcement investigative and intelligence activity. It provides mechanisms for controlling access to and dissemination of sensitive or classified information. Management of crisis information and intelligence is recognized under the NIMS as a sixth functional area within ICS. The structure of the JOC supports this functional area and enhances the overall management of critical incidents and special events.

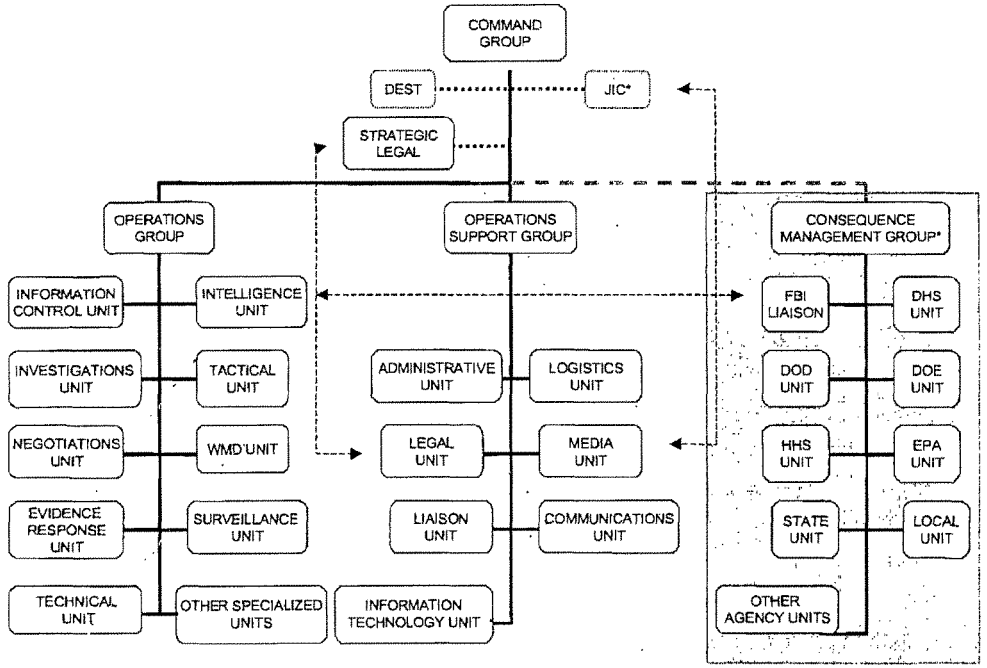
- The NIMS provides the framework within which the ICS and JOC structures operate for a unified approach to domestic incident management.

- The JOC is composed of four main groups: the Command Group, the Operations Group, the Operations Support Group, and the Consequence Management Group.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00222 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.163

FIGURE 2. Joint Operations Center



* While the Operations Group and Operations Support Group remain components of the JOC when it is incorporated into the JFO, the JIC and Consequence Management Group will be merged into the appropriate JFO staff components, if established.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00223 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC
46051.164

Command Group

- The Command Group of the JOC provides recommendations and advice to the FBI SAC regarding the development and implementation of strategic decisions to resolve the situation. It is responsible for approving the deployment and employment of law enforcement investigative and intelligence resources. The Command Group maintains its advisory role to the FBI SAC when the JOC becomes a section of the JFO for an Incident of National Significance. When a JFO is established in this situation, the FBI SAC becomes the SFLEO in the JFO Coordination Group. The Assistant SAC or an alternate senior FBI official leads the JOC Command Group once the SAC has transitioned to the JFO.

- The FBI representatives in the Command Group include the SAC, the Assistant SAC, and an executive-officer position known as the Crisis Management Coordinator (CMC). The SAC of the FBI Field Office in which the incident occurs is responsible for developing the overall strategy for managing Federal investigative law enforcement activities at the critical incident or special event and coordinating the implementation of that strategy with other agency decisionmakers and FBI Headquarters. The FBI SAC also is responsible for coordinating Federal law enforcement activities with other Federal incident management personnel during domestic critical incidents and special events. The CMC ensures that the strategy of the SAC is communicated to everyone in the JOC and that the JOC is staffed and equipped to effectively implement the strategy of the SAC. The CMC also ensures that information flows efficiently within the JOC and between the JOC and other command and control centers.

- The JOC Command Group includes senior officials with decisionmaking authority from local, State, and Federal agencies, as appropriate, based upon the circumstances of the threat or incident. Consistent with the Unified Command concept, law enforcement investigative and intelligence strategies, tactics, and priorities are determined jointly within the JOC Command Group. Federal law enforcement investigative, intelligence, and operational decisions are made cooperatively to the extent possible, but the authority to make these decisions rests ultimately with the FBI SAC.

- Three specialized teams provide guidance and expertise directly to the Command Group. These teams are the Strategic Legal Team, the Joint Information Center Team, and the Domestic Emergency Support Team.

  - The Strategic Legal Team is composed of legal counsel from the FBI, U.S. Attorney's Office, and the District or State's Attorney's Office. This team provides legal guidance to the Command Group concerning the strategies under consideration for resolution of the crisis.

  - The Joint Information Center (JIC) Team is integrated into the JFO when established. It is composed of the public affairs (media) officers from the participating local, State, and Federal public safety agencies. It manages information released to the public through a coordinated, unified approach. A separate media unit within the JOC Operations Support Group provides FBI-specific guidance and expertise to the FBI SAC and coordinates with the JIC to ensure the media strategy is consistent with the overall investigative strategy.

  - The Domestic Emergency Support Team (DEST) is a specialized interagency team composed of subject-matter experts from the FBI, the DHS/Emergency Preparedness and Response/Federal Emergency Management Agency (DHS/EPR/FEMA), DOD, DOE, HHS, and EPA. It provides guidance to the FBI SAC concerning WMD threats and actual incidents.

Operations Group

- The Operations Group handles all investigative, intelligence, and operational functions related to the threat, critical incident, or special event.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00224 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.165

- Each unit within the Operations Group provides expertise in a specific functional area that is important in the overall resolution of the incident.

- The units within the Operations Group are scalable and modular, and may be tailored to the specific threat, critical incident, or special event.

- The Operations Group normally consists of the Information Intake unit (formerly referred to as the Control unit), the Intelligence unit, the Investigations unit, and Field Operations units.

Information Intake (or Control)

- Information Intake is the central point for receiving all information that comes into the JOC. The purpose of Information Intake is to ensure that telephone calls, e-mail messages, fax reports, and other incoming information are assessed for relevance to the threat, critical incident, or special event. The information is checked to determine if it has been previously reported. It is prioritized and entered into the information management system. Through this filtering mechanism the Information Intake unit ensures that only current and relevant information is disseminated to the JOC.

- The Information Intake Coordinator is responsible for providing guidance and direction to all personnel within the Information Intake unit and coordinating the activities of the unit with all other units within the JOC. Personnel within the Information Intake unit are responsible for receiving incoming information, processing new information, routing followup information appropriately, and implementing procedures for tracking evidentiary material that is introduced into the command post.

Intelligence

- The Intelligence unit manages the collection, analysis, archiving, and dissemination of relevant and valid investigative and strategic intelligence. It fuses historical intelligence from a variety of sources with new intelligence specific to the threat, critical incident, or special event. The Intelligence unit also disseminates intelligence products and situation reports to all JOC units, FBI Headquarters Strategic Information and Operations Center (SIOC), and the JFO Coordination Group. This information is shared with the DHS Homeland Security Operations Center (HSOC), the National Counterterrorism Center (NCTC), and, as appropriate, other government agencies, consistent with operational security considerations.

- The Intelligence unit usually is divided into teams based on functional responsibility. Teams manage intelligence related to the crisis site or target, build intelligence portfolios and databases on significant elements related to the investigation (subjects, vehicles, and organizations), analyze and identify trends in activities related to the investigation (predictive and strategic intelligence), conduct liaison with outside members of the Intelligence Community, and prepare periodic briefings and reports concerning the status of the crisis or investigation. The Intelligence unit is responsible for collecting and reviewing all intelligence related to the threat, crisis, or special event to enable the SAC to further develop and refine strategic objectives.

Investigations

- The Investigations unit provides oversight and direction to all investigative activity related to the threat, critical incident, or special event. The Investigations unit implements the strategy of the SAC by directing the collection and management of investigative information. It is composed of investigative personnel from the agencies with specific jurisdiction or authority for investigating crimes related to the threat, critical incident, or special event. The Investigations Unit Coordinator is usually an FBI Supervisor who has responsibility for investigating the most significant substantive law violation.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00225 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.166

- Teams within the Investigations unit review all incoming information to determine investigative value. The Investigations unit assigns, tracks, and reviews all investigative leads and documents the investigation in the appropriate case file(s). The case agents or primary investigators within the Investigations unit manage all evidence and information, and prepare it for court presentation, if appropriate. The case agents or primary investigators are assisted by analytical personnel to ensure that all investigative information is pursued to its logical conclusion. A Records Check Team within the Investigations unit reviews case files and databases to ensure that all items of investigative value are identified and evaluated. The Investigations unit is responsible for collecting and reviewing all reports of investigative activity to enable the SAC to further develop and refine strategic objectives.

Field Operations

- The Field Operations units are based upon the specific needs of the threat, critical incident, or special event. The personnel staffing these units are subject-matter experts in a number of specialized skill areas. Field Operations unit coordinators are responsible for ensuring the activity of the specialized units is consistent with and in support of the strategy of the SAC.

- Field Operations units may include representatives of tactical, negotiations, WMD/CBRNE, evidence response, surveillance, technical, or any other specialized unit deployed to the crisis site(s) or staged in readiness. The mission of these units is to provide the SAC with current information and specialized assistance in dealing with the threat, critical incident, or special event. Information is communicated between the JOC and the crisis site(s) through the Field Operations unit representatives in the JOC. This ensures that decisionmakers both in the JOC and in the forward areas maintain full situational awareness. The Field Operations units coordinate their activities within the JOC to ensure each is aware of the impact of their activities on the other field units.

- Local, State, and Federal law enforcement specialty units assigned to assist with field operations during the threat, incident, or special event coordinate their activities with the appropriate FBI Field Operations units through the JOC. Federal Government mission-specific units are designated to help the FBI maintain their respective chains of command and coordinate their activities through representation in the JOC. The JOC manages the activities of the specialized units at a strategic level. Activities at the individual or "tactical" level are managed at the crisis site(s) through forward command structures such as the Tactical Operations Center, Negotiations Operations Center, and Evidence Response Team Operations Center.

Operations Support Group

- The Operations Support Group units designated within the JOC are based upon the specific needs of the threat, critical incident, or special event. The personnel who staff these units are subject-matter experts in a number of specialized areas. Operations Support Group unit coordinators are responsible for ensuring the activity of their units is consistent with and in support of the strategy of the SAC.

- Operations Support Group units can include administrative, logistics, legal, media, liaison, communications, and information management. The mission of these units is to support the investigative, intelligence, and operational functions of the JOC.

- The Administrative and Logistics units have responsibilities that are similar to the Finance and Logistics Sections in ICS. However, they are tasked with managing only the activities related to the law enforcement investigative, intelligence, and operational functions; they do not manage the administrative and logistics functions associated with the overall incident.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00226 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.167

- The Legal and Media units support the investigative and intelligence operations of the JOC through the preparation of specific legal processes and management of media affairs. These units focus on specific objectives related to the investigation such as search warrants and press releases, and not the strategic overall objectives handled by the Strategic Legal Team and JIC that are attached to the Command Group.

- The Liaison unit is composed of representatives from outside agencies who assist the FBI with resolution of the threat, critical incident, or special event. The Liaison unit may include agencies without clear authority or jurisdiction over the threat, critical incident, or special event if they have a potential investigative interest. For example, law enforcement agencies that border affected jurisdictions may be represented in the JOC to maintain situational awareness of potential threats. Additional Liaison unit representatives may include fire department personnel, utility company workers, or engineering specialists.

- The Communications unit handles radio and telephone communications to support JOC operations. The Communications unit establishes communications networks within the JOC. It also establishes networks to facilitate timely and reliable information-sharing between the JOC and other command and control centers.

- The Information Technology unit is responsible for the JOC computer system operation within each unit and between units. Information technology specialists and facilitators assigned to this unit are responsible for ensuring the uninterrupted operation of the information management system used during JOC operations.

Consequence Management Group

- The JOC Consequence Management Group consists of representatives of agencies that provide consequence-focused expertise in support of law enforcement activities. The JOC does not manage consequence functions; rather, it ensures that law enforcement activities with emergency management implications are communicated and coordinated to appropriate personnel in a complete and timely manner.

- A DHS representative coordinates the actions of the JOC Consequence Management Group, and expedites activation of a Federal incident management response should it become necessary. FBI and DHS representatives screen threat/incident intelligence for the Consequence Management Group. Representatives of the JOC Consequence Management Group monitor the law enforcement criminal investigation and may provide advice regarding decisions that impact the general public or critical infrastructure. This integration provides continuity should a Federal incident management response become necessary.

- Agencies comprising the Consequence Management Group may also have personnel assigned to other units within the JOC structure. Depending on the nature of the incident and required assets, additional teams assigned to support the FBI may be included under Other Specialized Units.

- Should the threat of a terrorist incident become imminent, the JOC Consequence Management Group may forward recommendations to the RRCC Director to initiate limited pre-deployment of assets under the Stafford Act.

- Requests for DOD assistance for law enforcement and criminal investigation during the incident come from the Attorney General to the Secretary of Defense through the DOD Executive Secretary. Once the Secretary approves the request, the order is transmitted either directly to the unit involved or through the Chairman of the Joint Chiefs of Staff. The FBI SAC informs the Principal Federal Official (PFO), if one has been designated, when requesting this additional assistance.

- The Consequence Management Group is established when a JOC is necessary but a JFO has not yet been activated, or the event has not reached the level of being considered an Incident of National Significance.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00227 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.168

- Representatives in this group may move to appropriate positions in other sections of the JFO when one is established.

The Response

- Receipt of a terrorist threat may be through any source or medium and may be articulated or developed through intelligence sources. It is the responsibility of all local, State, and Federal agencies and departments to notify the FBI when such a threat is received. As explained below, the FBI evaluates the credibility of the terrorist threat and notifies the HSOC, NCTC, and other departments and agencies, as appropriate.

- Upon receipt of a threat of terrorism within the United States, the FBI conducts a formal threat credibility assessment in support of operations with assistance from select interagency experts. For a WMD or CBRNE threat, this assessment includes three perspectives:

  - Technical Feasibility: An assessment of the capacity of the threatening individual or organization to obtain or produce the material at issue;

  - Operational Practicability: An assessment of the feasibility of delivering or employing the material in the manner threatened; and

  - Behavioral Resolve: A psychological assessment of the likelihood that the subject(s) will carry out the threat, including a review of any written or verbal statement by the subject(s).

- A threat assessment is conducted to determine whether the potential threat is credible, and confirm whether WMD or CBRNE materials are involved in the developing terrorist incident. Intelligence varies with each threat and impacts the level of the Federal response. If the threat is credible, the situation requires the tailoring of response actions to use Federal resources needed to anticipate, prevent, and/or resolve the situation. The Federal response focuses on law enforcement/investigative actions taken in the interest of public safety and welfare, and is predominantly concerned with preventing and resolving the threat. In addition, contingency planning focuses on the response to potential consequences and the pre-positioning of tailored resources, as required. The threat increases in significance when the presence of a CBRNE device or WMD capable of causing a significant destructive event, prior to actual injury or loss, is confirmed or when intelligence and circumstances indicate a high probability that a device exists. In this case, the threat has developed into a WMD or CBRNE terrorist situation requiring an immediate process to identify, acquire, and plan the use of Federal resources to augment State, local, and tribal authorities in lessening or averting the potential consequence of terrorist use or employment of WMD or CBRNE material. It should be noted that a threat assessment would also be conducted if an incident occurs without warning. In this case, the assessment is focused on criminal intent, the extent of the threat, and the likelihood of secondary devices or locations.

- The FBI manages a Terrorist Threat Warning System to ensure that vital information regarding terrorism reaches those in the U.S. counterterrorism and law enforcement community responsible for countering terrorist threats. This information is coordinated with DHS and the NCTC, and is transmitted via secure teletype. Each message transmitted under this system is an alert, an advisory, or an assessment—an alert if the terrorist threat is credible and specific, an advisory if the threat is credible but general in both timing and target, or an assessment to impart facts and/or threat analysis concerning terrorism.

- Upon determination of a credible threat, FBI Headquarters activates its SIOC to coordinate and manage the national-level support to a terrorism incident. At this level, the SIOC generally mirrors the JOC structure operating in the field. The SIOC is staffed by liaison officers from other Federal agencies who coordinate with and provide assistance to the FBI. The SIOC serves as the focal point for law enforcement operations and maintains direct connectivity with the HSOC. The HSOC is notified immediately by the SIOC once a threat has been determined to be credible. In turn, this notification may result in activation of NRP components in coordination with the FBI.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00228 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.169

- The FBI leads the criminal investigation related to the incident, and the SIOC is the focal point for all intelligence related to the investigative law enforcement response to the incident. Consistent with the NRP, affected Federal agencies operate headquarters-level emergency operations centers, as necessary. FBI Headquarters initiates appropriate liaison with other Federal agencies to activate their operations centers and provide liaison officers to the SIOC. In addition, FBI Headquarters initiates communications with the SAC of the responsible Field Office, apprising him/her of possible courses of action and discussing deployment of the DEST. The FBI SAC establishes initial operational priorities based upon the specific circumstances of the threat or incident. This information is then forwarded to FBI Headquarters to coordinate identification and deployment of appropriate resources.

- The JOC is established by the FBI under the operational control of the FBI SAC, and acts as the focal point for the field coordination of criminal investigation, law enforcement, and intelligence activities related to the threat or incident. When a PFO is designated for a terrorism incident, the FBI SAC provides full and prompt cooperation, resources, and support to the PFO, as appropriate and consistent with applicable authorities. The PFO (or an initial PFO designated by the Secretary of Homeland Security) may elect to use the JOC as an initial operating facility for strategic management and identification of State, local, and tribal requirements and priorities, and coordination of the Federal response. The FBI SAC coordinates with the PFO, including providing incident information to the PFO as requested, coordinating the public communications strategy with the PFO, and approving Federal interagency communications for release to the public through the PFO. It is recognized, however, that in some cases it may be necessary for the FBI SAC to respond directly to media/public inquiries on investigative operations and matters affecting law enforcement operations, particularly during the early stages of the emergency response.

- The local FBI Field Office activates a Crisis Management Team to establish the JOC in the affected area, possibly collocated with an existing emergency operations facility. In locating the JOC, consideration is given to the possibility that the facility may have to accommodate other Federal incident management field activities including the JFO, the JIC, and other supporting teams. Additionally, the JOC is augmented by outside agencies, including representatives from the DEST (if deployed), who provide interagency technical expertise as well as interagency continuity during the transition from an FBI command post structure to the JOC structure.

- Based upon a credible threat assessment and a request by the SAC, the FBI Director and DHS Under Secretary for Emergency Preparedness and Response, in consultation with the Attorney General and Secretary of Homeland Security, may request authorization through the National Security Council to deploy the DEST to assist the SAC in mitigating the crisis situation. The DEST is a rapidly deployable, interagency team responsible for providing expert advice and support concerning the Federal Government's capabilities in resolving the terrorist threat or incident. This includes law enforcement, criminal investigation, and emergency management assistance, technical and scientific advice, and contingency planning guidance tailored to situations involving chemical, biological, or nuclear/radiological weapons.

- Upon arrival at the FBI command post or JOC, the DEST may act as a stand-alone advisory team to the SAC providing recommended courses of action. Although it would be unusual, the DEST may be tasked to deploy before a JOC is established. The DEST may handle some of the specialized interagency functions of the JOC until the JOC is fully staffed. The DEST emergency management component merges into the Consequence Management Group in the JOC structure.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00229 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.170

- Prior to an actual WMD or CBRNE incident, law enforcement, intelligence, and investigative activities generally have priority. When an incident results in the use of WMD or CBRNE material, rescue and life-safety activities generally bave priority. Activities may overlap and/or run concurrently during the incident management, and are dependent on the threat and/or the strategies for responding to the incident.

- Upon determination that applicable law enforeement/intelligence goals and objectives are met and no further immediate threat exists, the FBI SAC may deactivate the JOC and order a return to routine law enforcement/investigative operations in accordance with pre-event protocols.

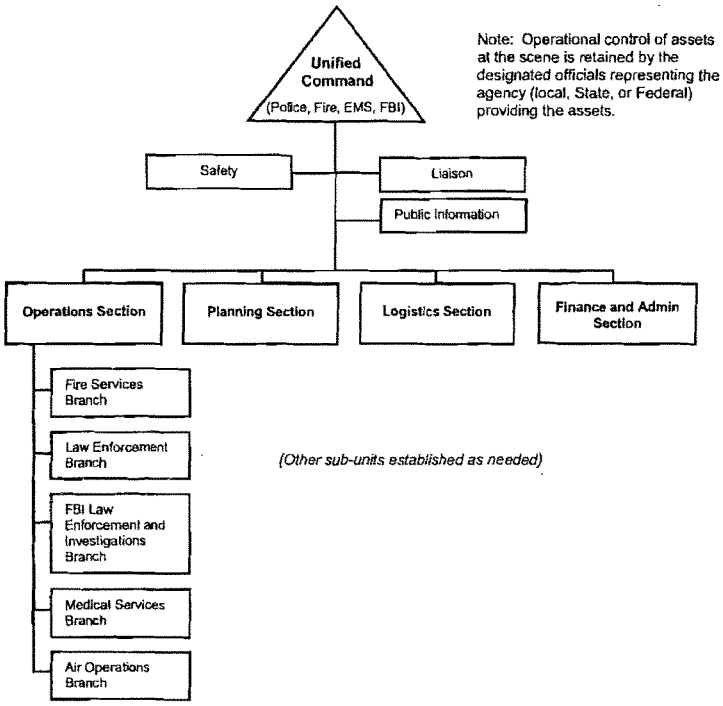
- When an incident occurs and an ICP is established on-scene, FBI personnel integrate into the ICP to enhance the ability of the FBI to carry out its mandated mission (see Figure 3). Three specific positions within an ICP are provided. The first FBI Special Agent (SA) or Joint Terrorism Task Force (JTTF) member responding receives an initial briefing from the Incident Commander or his/her designee and works closely with the Incident Commander as a member of the Unified Command. The FBI representative then informs the local Field Office of the current situation and, if necessary, requests additional assets. When a more senior FBI SA arrives on the scene, he/she assumes the role of the FBI representative in the Unified Command.

- The first arriving SA or JTTF member moves to the Operations Section as the Deputy Chief of Operations. This position is responsible for managing the deployment and coordination of Federal law enforcement and investigative assets in support of the Incident Action Plan. Additionally, an FBI SA assumes the position of Deputy Chief of Planning within the ICP. This position permits the FBI SA to remain updated on the situation and serve as a conduit for requests for additional law enforcement and investigative assets. The Agent also inputs Federal objectives into the developing incident action plan and performs other duties as appropriate. Also, FBI assets form a unit in the Operations Section. Throughout the incident, the actions and activities of the Unified Command at the incident scene and the Command Group of the JOC (and the JFO Coordination Group if established) are continuously and completely coordinated throughout the incident.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00230 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.171

FIGURE 3. On-scene coordination



VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00231 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.172

ENCLOSURE C

2. Nuclear/Radiological Incident Annex

Nuclear/Radiological Incident Annex

Coordinating Agencies:

Department of Defense
Department of Energy
Department of Homeland Security
Environmental Protection Agency
National Aeronautics and Space Administration
Nuclear Regulatory Commission

Cooperating Agencies:

Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of Housing and Urban Development
Department of the Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of Veterans Affairs
Environmental Protection Agency
General Services Administration
Nuclear Regulatory Commission
American Red Cross

Introduction

Purpose

The Nuclear/Radiological Incident Annex provides an organized and integrated capability for a timely, coordinated response by Federal agencies to terrorist incidents involving nuclear or radioactive materials (Incidents of National Significance), and accidents or incidents involving such material that may or may not rise to the level of an Incident of National Significance. The Department of Homeland Security (DHS) is responsible for overall coordination of all actual and potential Incidents of National Significance, including terrorist incidents involving nuclear materials.

This annex describes how the coordinating agencies and cooperating agencies support DHS's overall coordination of the response to a nuclear/radiological Incident of National Significance. In addition, this annex describes how the coordinating agencies lead the response to incidents of lesser severity. [1]

The actions described in this annex may be implemented: (1) concurrently with, and as an integral part of, the National Response Plan (NRP) for all nuclear/radiological incidents or accidents considered to be Incidents of National Significance; or (2) independently for all other nuclear/radiological accidents or incidents considered to be below the threshold of an Incident of National Significance and, therefore, not requiring overall Federal coordination by DHS.

[1] Nuclear/radiological incidents of "lesser severity" are considered below the threshold of an Incident of National Significance, as determined by DHS, and vary from lost radiography sources or discovery of orphan radiological sources to incidents/emergencies at nuclear power plants below the classification of General Emergency, as defined by the cognizant regulatory agency (e.g., Department of Energy (DOE) or Nuclear Regulatory Commission (NRC)).

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00233 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.174

Scope

This annex applies to nuclear/radiological incidents, including sabotage and terrorist incidents, involving the release or potential release of radioactive material that poses an actual or perceived hazard to public health, safety, national security, and/or the environment. This includes terrorist use of radiological dispersal devices (RDDs) or improvised nuclear devices (INDs) as well as reactor plant accidents (commercial or weapons production facilities), lost radioactive material sources, transportation accidents involving nuclear/ radioactive material, and foreign accidents involving nuclear or radioactive material.

The level of Federal response to a specific incident is based on numerous factors, including the ability of State, local, and tribal officials to respond; the type and/or amount of radioactive material involved; the extent of the impact or potential impact on the public and environment; and the size of the affected area.

In situations where threat analysis includes indications that a terrorist incident involving radiological materials could occur, actions are coordinated in accordance with the pre-incident prevention protocols set forth in the NRP Base Plan.

This annex:

- Provides planning guidance and outlines operational concepts for the Federal response to any nuclear/radiological incident, including a terrorist incident, that has actual, potential, or perceived radiological consequences within the United States or its territories, possessions, or territorial waters, and that requires a response by the Federal Government. This includes both Incidents of National Significance and incidents of lesser severity;
- Acknowledges the unique nature of a variety of nuclear/radiological incidents and the responsibilities of Federal, State, local, and tribal governments to respond to them;
- Describes Federal policies and planning considerations on which this annex and Federal agency-specific nuclear/radiological response plans are based;
- Specifies the roles and responsibilities of Federal agencies for preventing, preparing for, responding to, and recovering from nuclear/radiological incidents;
- Includes guidelines for notification, coordination, and leadership of Federal activities, and coordination of public information, congressional relations, and international activities; and
- Provides protocols for coordinating Federal Government capabilities to respond to radiological incidents. These capabilities include, but are not limited to:
  - The Interagency Modeling and Atmospheric Assessment Center (IMAAC), which is responsible for production, coordination, and dissemination of consequence predictions for an airborne hazardous material release;
  - The Federal Radiological Monitoring and Assessment Center (FRMAC), established at or near the scene of an incident to coordinate radiological assessment and monitoring; and
  - The Advisory Team for Environment, Food, and Health (known as "the Advisory Team"), which provides expert recommendations on protective action guidance.

More information on these capabilities is included in subsequent sections of this annex.

Policies

- DHS coordinates the overall Federal Government response to radiological Incidents of National Significance in accordance with Homeland Security Presidential Directive-5 and the NRP. In the NRP Base Plan, Figure 4, Structure for NRP Coordination: Terrorist Incident, illustrates the organizational framework that DHS utilizes to respond to terrorist incidents. In the NRP Base Plan, Figure 5, Structure for NRP Coordination: Federal-to-Federal Support, illustrates the organizational framework that DHS utilizes to respond to nonterrorist Incidents of National Significance.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00234 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.175

- The NRP supersedes the Federal Radiological Emergency Response Plan, dated May 1, 1996.

- The concept of operations described in this annex recognizes and addresses the unique challenges associated with and the need for specialized technical expertise/actions when responding to RDD/IND incidents with potentially catastrophic consequences.

- DHS, as the overall incident manager for Incidents of National Significance, is supported by coordinating agencies and cooperating agencies. Coordinating agencies have specific nuclear/radiological technical expertise and assets for responding to the unique characteristics of these types of incidents. Coordinating agencies facilitate the nuclear/radiological aspects of the response in support of DHS. For any given incident, the coordinating agency is the Federal agency that owns, has custody of, authorizes, regulates, or is otherwise designated responsibility for the nuclear/radioactive material, facility, or activity involved in the incident. The coordinating agency is represented in the Joint Field Office (JFO) Coordination Group, the Interagency Incident Management Group (IIMG), and the Homeland Security Operations Center (HSOC). The coordinating agency is also represented in other response centers and entities, as appropriate for the specific incident.

- Coordinating agencies are also responsible for leading the Federal response to nuclear/radiological incidents of lesser severity (those incidents that do not reach the level of an Incident of National Significance).

- Coordinating agencies may use the structure of the NRP to carry out their response duties, or any other structure consistent with the National Incident Management System (NIMS) capable of providing the required support to the affected State, local, or tribal government.

- Cooperating agencies include other Federal agencies that provide technical and resource support to DHS and the coordinating agencies. These agencies are represented in the IIMG, the HSOC, and other response centers and entities, as appropriate for the specific incident. They may or may not be represented in the JFO Coordination Group.

- DHS/Emergency Preparedness and Response/Federal Emergency Management Agency (DHS/EPR/FEMA) is responsible for maintaining and updating this annex. DHS/EPR/FEMA accomplishes this responsibility through the Federal Radiological Preparedness Coordinating Committee (FRPCC).

- The Attorney General, generally acting through the Federal Bureau of Investigation (FBI), has lead responsibility for criminal investigations of terrorist acts or terrorist threats and for coordinating activities of other members of the law enforcement community to detect, prevent, preempt, investigate, and disrupt terrorist attacks against the United States, including incidents involving nuclear/radioactive materials, in accordance with the following:

  - The Atomic Energy Act directs the FBI to investigate all alleged or suspected criminal violations of the act. Additionally, the FBI legally is responsible for locating any illegally diverted nuclear weapon, device, or material and for restoring nuclear facilities to their rightful custodians. In view of its unique responsibilities under the Atomic Energy Act (amended by the Energy Reorganization Act), the FBI has concluded formal agreements with the coordinating agencies that provide for interface, coordination, and technical support for the FBI's law enforcement and criminal investigative efforts.

  - Generally, for nuclear facilities and materials in transit, the designated coordinating agency and cooperating agencies perform the functions delineated in this annex and provide technical support and assistance to the FBI in the performance of its law enforcement and criminal investigative mission. Those agencies supporting the FBI additionally coordinate and manage the technical portion of the response and activate/request assistance under this annex for measures to protect the public health and safety. In all cases, the

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00235 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.176

FBI manages and directs the law enforcement and intelligence aspects of the response, while coordinating its activities with appropriate Federal, State, local, and tribal governments within the framework of this annex, and/or as provided for in established interagency agreements or plans. Further details regarding the FBI response are outlined in the Terrorism Incident Law Enforcement and Investigation Annex.

- All Federal nuclear/radiological assistance capabilities outlined in this annex are available to support the Federal response to a terrorist threat, whether or not the threat develops into an actual incident.

- When the concept of operations in this annex is implemented, existing interagency plans that address nuclear/radiological incident management are incorporated as supporting plans and/or operational supplements (e.g., the National Oil and Hazardous Substances Pollution Contingency Plan (NCP)).

- This annex does not create any new authorities nor change any existing ones.

- Nothing in this annex alters or impedes the ability of Federal departments and agencies to carry out their specific authorities and perform their responsibilities under law.

- Some Federal agencies are authorized to respond directly to certain incidents affecting public health and safety. In these cases, procedures outlined in this annex may be used to coordinate the delivery of Federal resources to State, local, and tribal governments, and to coordinate assistance among Federal agencies for incidents that can be managed without the need for DHS coordination (i.e., incidents below the threshold of an Incident of National Significance).

- The owner/operator of a nuclear/radiological facility primarily is responsible for mitigating the consequences of an incident, providing notification and appropriate protective action recommendations to State, local, and/or tribal government officials, and minimizing the radiological hazard to the public. The owner/operator has primary responsibility for actions within the facility boundary and may also have responsibilities for response and recovery activities outside the facility boundary under applicable legal obligations (e.g., contractual; licensee; Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA)).

- State, local, and tribal governments primarily are responsible for determining and implementing measures to protect life, property, and the environment in those areas outside the facility boundary or incident location. This does not, however, relieve nuclear/radiological facility or material owners/operators from any applicable legal obligations.

- State, local, and tribal governments and owners/operators of nuclear/radiological facilities or activities may request assistance directly from DHS, other Federal agencies, and/or State governments with which they have preexisting arrangements or relationships.

- Response to nuclear/radiological incidents affecting land owned by the Federal Government is coordinated with the agency responsible for managing that land to ensure that incident management activities are consistent with Federal statutes governing use and occupancy. In the case of tribal lands, tribal governments have a special relationship with the U.S. Government, and Federal, State, and local governments may have limited or no authority on specific tribal reservations. Further guidance is provided in the Tribal Relations Support Annex.

- Participating Federal agencies may take appropriate independent emergency actions within the limits of their own statutory authority to protect the public, mitigate immediate hazards, and gather information concerning the emergency to avoid delay.

- Departments and agencies are not reimbursed for activities conducted under their own authorities unless other agreements or reimbursement mechanisms exist (e.g., Stafford Act, Federal-to-Federal assistance).

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00236 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.177

- Federal coordination centers and agency teams provide their own logistical support consistent with agreed upon interagency execution plans. State, local, and tribal governments are encouraged to coordinate their efforts with the Federal effort, but maintain their own logistical support, consistent with applicable authorities and requirements.

- For radiological incidents involving a nuclear weapon, special nuclear material, and/or classified components, the agency with custody of the material (the Department of Defense (DOD), the Department of Energy (DOE), or the National Aeronautics and Space Administration (NASA)) may establish a National Defense Area (NDA) or National Security Area (NSA). NDAs and NSAs are established to safeguard classified information and/or restricted data, or equipment and material, and place non-Federal lands under Federal control for the duration of the incident. In the event radioactive contamination occurs, Federal officials coordinate with State and local officials to ensure appropriate public health and safety actions are taken outside the NDA or NSA.

Planning Assumptions

- Radiological incidents may not be immediately recognized as such until the radioactive material is detected or the effects of radiation exposure are manifested in the population.

- An act of radiological terrorism, particularly an act directed against a large population center within the United States, will have major consequences that can overwhelm the capabilities of many local, State, and/or tribal governments to respond and may seriously challenge existing Federal response capabilities.

- A radiological incident may include chemical or biological contaminants, which may require concurrent implementation of the NCP or other Federal plans and procedures.

- An incident involving the potential release of radioactivity may require implementation of protective measures.

- An expeditious Federal response is required to mitigate the consequences of the nuclear/radiological incident. Radiological Incidents of National Significance that result in significant impacts likely will trigger implementation of the NRP Catastrophic Incident Annex and Catastrophic Incident Supplement.

- The Federal Government response to radiological terrorist threats/incidents also includes the following assumptions:

  - If appropriate personal protective equipment and capabilities are not available and the area is contaminated by radioactive material, response actions in a contaminated area may be delayed until the material has dissipated to a safe level for emergency response personnel or until appropriate personal protective equipment and capabilities arrive, whichever is sooner;

  - The response to a radiological threat or actual incident requires an integrated Federal Government response;

  - In the case of a radiological terrorist attack, the effect may be temporarily and geographically dispersed, requiring response operations to be conducted over a multijurisdictional, multistate region; and

  - A radiological terrorist incident may affect a single location, or multiple locations, each of which may require an incident response and a crime scene investigation simultaneously.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00237 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.178

Concept of Operations

General

This concept of operations is applicable to potential and actual radiological Incidents of National Significance requiring DHS coordination and other radiological incidents of lesser severity, utilizing the protocols delineated in this annex. For other radiological incidents of lesser severity, other Federal response plans (i.e., the NCP and/or agency-specific radiological incident response plans) may also be utilized, as appropriate.

Hazard-Specific Planning and Preparedness

Headquarters

- The Federal Radiological Policy Coordinating Committee (FRPCC) provides a national-level forum for the development and coordination of radiological prevention and preparedness policies and procedures. It also provides policy guidance for Federal radiological incident management activities in support of State, local and tribal government radiological emergency planning and preparedness activities. The FRPCC is an interagency body consisting of the coordinating and cooperating agencies discussed in this annex, chaired by DHS/EPR/FEMA. The FRPCC establishes subcommittees, as necessary.

- The FRPCC also coordinates research-study efforts of its member agencies related to State, local and tribal government radiological emergency preparedness to ensure minimum duplication and maximum benefits to State and local governments. The FRPCC coordinates planning and validating requirements of each agency, reviewing integration requirements and incorporating agency-specific plans, procedures, and equipment into the response system.

Regional: Regional Assistance Committees (RACs) in the DHS/EPR/FEMA regions serve as the primary coordinating structure at the Federal regional level. RAC membership mirrors that of the FRPCC, and RACs are chaired by a DHS/EPR/FEMA regional representative. Additionally, State emergency management agencies send representatives to RAC meetings and participate in regional exercise and training activities. The RACs provide a forum for information-sharing, consultation, and coordination of Federal regional awareness, prevention, preparedness, response, and recovery activities. The RACs also assist in providing technical assistance to State and local governments and evaluating radiological plans and exercises.

Coordinating Agencies and Cooperating Agencies

During a response to an Incident of National Significance, coordinating agencies and cooperating agencies provide technical expertise, specialized equipment, and personnel in support of DHS, which is responsible for overall coordination of incident management activities. Coordinating agencies have primary responsibilities for Federal activities related to the nuclear/radiological aspects of the incident.

The coordinating agency is that Federal agency which owns, has custody of, authorizes, regulates, or is otherwise deemed responsible for the radiological facility or activity involved in the incident. The following paragraphs identify the coordinating agency for a variety of radiological incidents. For example, the Nuclear Regulatory Commission (NRC) is the coordinating agency for incidents involving nuclear facilities licensed by the NRC; DOE is the coordinating agency for incidents involving the transportation of radioactive materials shipped by or for DOE. Table 1 identifies the coordinating agency for a variety of radiological incidents.

Radiological Terrorism Incidents:

- The coordinating agency provides technical support to DHS, which has overall responsibility for domestic incident management, and to the FBI, which has the lead responsibility for criminal investigations of terrorist acts or terrorist threats. The FBI also is responsible for coordinating activities of other members of the law enforcement community to detect, prevent, preempt, investigate, and disrupt terrorist attacks against the United States, including incidents involving nuclear/radioactive materials (e.g. RDD/IND incidents).

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00238 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.179

TABLE 1. Coordinating agencies

Note: DHS is responsible for the overall coordination of incident management activities for all nuclear or radiological Incidents of National Significance, including those involving terrorism.

Type of Incident	Coordinating Agency
a. Radiological terrorism incidents (e.g., RDD/IND or radiological exposure device):	
(1) Material or facilities owned or operated by DOD or DOE	(1) DOD or DOE
(2) Material or facilities licensed by NRC or Agreement State	(2) NRC
(3) All others	(3) DOE
b. Nuclear facilities:	
(1) Owned or operated by DOD or DOE	(1) DOD or DOE
(2) Licensed by NRC or Agreement State	(2) NRC
(3) Not licensed, owned, or operated by a Federal agency or an Agreement State, or currently or formerly licensed facilities for which the owner/operator is not financially viable or is otherwise unable to respond	(3) EPA
c. Transportation of radioactive materials:	
(1) Materials shipped by or for DOD or DOE	(1) DOD or DOE
(2) Shipment of NRC or Agreement State-licensed materials	(2) NRC
(3) Shipment of materials in certain areas of the coastal zone that are not licensed or owned by a Federal agency or Agreement State (see USCG list of responsibilities for further explanation of "certain areas")	(3) DHS/USCG
(4) All others	(4) EPA
d. Space vehicles containing radioactive materials:	
(1) Managed by NASA or DOD	(1) NASA or DOD
(2) Not managed by DOD or NASA impacting certain areas of the coastal zone	(2) DHS/USCG
(3) All others	(3) EPA
e. Foreign, unknown or unlicensed material:	
(1) Incidents involving foreign or unknown sources of radioactive material in certain areas of the coastal zone	(1) DHS/USCG
(2) All others	(2) EPA
f. Nuclear weapon accident/incident (based on custody at time of event)	DOD or DOE
Other types of incidents not otherwise addressed above	DHS designates

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00239 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.180

- For radiological terrorism incidents involving materials or facilities owned or operated by DOD or DOE, DOD or DOE is the coordinating agency, as appropriate.

- For radiological terrorism incidents involving materials or facilities licensed by the NRC or Agreement States, the NRC is the coordinating agency.

- For all other radiological terrorist incidents, DOE is the coordinating agency. The coordinating agency role transitions from DOE to the Environmental Protection Agency (EPA) for environmental cleanup and site restoration at a mutually agreeable time, and after consultation with State, local, and tribal governments, the cooperating agencies, and the JFO Coordination Group.

Nuclear Facilities:

- The NRC is the coordinating agency for incidents that occur at fixed facilities or activities licensed by the NRC or an Agreement State. These include, but are not limited to, commercial nuclear power plants, fuel cycle facilities, DOE-owned gaseous diffusion facilities operating under NRC regulatory oversight, independent spent fuel storage installations, radiopharmaceutical manufacturers, and research reactors.

- DOD or DOE is the coordinating agency for incidents that occur at facilities or vessels under their jurisdiction, custody, or control. These incidents may involve reactor operations, nuclear material, weapons production, radioactive material from nuclear weapons or munitions, or other radiological activities.

- EPA is the coordinating agency for incidents that occur at facilities not licensed, owned, or operated by a Federal agency or an Agreement State, or currently or formerly licensed facilities for which the owner/operator is not financially viable or is otherwise unable to respond.

Transportation of Radioactive Materials:

- Either DOD or DOE is the coordinating agency for transportation incidents involving DOD or DOE materials, depending on which of these agencies has custody of the material at the time of the incident.

- The NRC is the coordinating agency for transportation incidents that involve radiological material licensed by the NRC or an Agreement State.

- DHS/U.S. Coast Guard (DHS/USCG) is the coordinating agency for the shipment of materials in certain areas of the coastal zone that are not licensed or owned by a Federal agency or Agreement State.

- EPA is the coordinating agency for shipment of materials in other areas of the coastal zone and in the inland zone that are not licensed or owned by a Federal agency or an Agreement State.

Space Vehicles Containing Radioactive Materials:

- NASA is the coordinating agency for missions involving NASA space vehicles or joint space vehicles with significant NASA involvement. DOD is the coordinating agency for missions involving DOD space vehicles or joint space vehicles with significant DOD involvement. A joint venture is an activity in which the U.S. Government has provided extensive design/financial input; has provided and maintains ownership of instruments, spacecraft, or the launch vehicle; or is intimately involved in mission operations. A joint venture is not created by simply selling or supplying material to a foreign country for use in its spacecraft.

- DHS/USCG is the coordinating agency for space vehicles not managed by DOD or NASA impacting certain areas of the coastal zone.

- EPA is the coordinating agency for all other space vehicle incidents involving radioactive material.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00240 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.181

Foreign, Unknown, or Unlicensed Material: EPA or DHS/USCG is the coordinating agency depending on the location of the incident. DHS/USCG is the coordinating agency for incidents involving foreign or unknown sources of radioactive material in certain areas of the coastal zone. EPA is the coordinating agency for all other incidents involving foreign, unknown, or unlicensed radiological sources that have actual, potential, or perceived radiological consequences in the United States or its territories, possessions, or territorial waters. The foreign or unlicensed source may be a reactor, a spacecraft containing radioactive material, imported radioactively contaminated material, or a shipment of foreign-owned radioactive material. Unknown sources of radioactive material, also termed "orphan sources," are those materials whose origin and/or radiological nature are not yet established. These types of sources include contaminated scrap metal or abandoned radioactive material.

Other Types of Incidents: For other types of incidents not covered above, DHS, in consultation with the other coordinating agencies, designates a coordinating agency. If DHS determines that it is an Incident of National Significance, DHS is responsible for overall coordination and the designated coordinating agency assumes responsibilities as the coordinating agency.

Notification Procedures

- The owner/operator of a nuclear/radiological facility or owner/transporter of nuclear/radiological material is generally the first to become aware of an incident and notifies State, local and tribal authorities and the coordinating agency.
- Federal, State, local, and tribal governments that become aware of a radiological incident from any source other than the coordinating agency notify the HSOC and the coordinating agency.
- The coordinating agency provides notification of a radiological incident to the HSOC and other coordinating agencies, as appropriate.
- Releases of hazardous materials that are regulated under the NCP (40 CFR part 302) are reported to the National Response Center.

Incident Actions

Headquarters: Incidents of National Significance

- Coordinating agencies and cooperating agencies report information and intelligence relative to situational awareness and incident management to the HSOC. Agencies with radiological response functions provide representatives to the HSOC, as requested.
- The coordinating agency and cooperating agencies, as appropriate, provide representation to the IIMG.
- Coordinating agencies and cooperating agencies provide representation to the National Response Coordination Center (NRCC), as appropriate.

Other Radiological Incidents

- For radiological incidents that are below the threshold of an Incident of National Significance but require Federal participation in the response, the coordinating agency coordinates the Federal response utilizing the procedures in this annex, agency-specific plans, and/or the NCP, as appropriate. The coordinating agency provides intelligence and information relative to the incident to the HSOC.
- The NRCC may be utilized to provide interagency coordination and Federal resource tracking, if needed.

Regional: Incidents of National Significance

- The coordinating agency provides representation to the JFO to serve as a Senior Federal Official within the JFO Coordination Group. Cooperating agencies may also be represented, as needed.
- The coordinating agency is part of the Unified Command, as defined by the NIMS, and coordinates Federal radiological response activities at appropriate field facilities.[2]

[2] Appropriate field facilities may include a JFO, Incident Command Post, Emergency Operations Center, Emergency Operations Facility, Emergency Control Center, etc.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00241 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.182

Other Radiological Incidents: The coordinating agency coordinates Federal response operations at a designated field facility. Cooperating agencies may also be represented, as needed.

Response Functions: Primary radiological response functions are addressed in this section. An overview of specific DHS and coordinating agency response functions is provided in Table 2.

Table 2: DHS and coordinating agency response functions overview

Response Function	Incidents of National Significance	Other Radiological Incidents
a. Coordinate actions of Federal agencies related to the overall response.	DHS	Coordinating agency
b. Coordinate Federal activities related to response and recovery of the radiological aspects of an incident.	DHS and coordinating agency	Coordinating agency
c. Coordinate incident security.	DHS and coordinating agency	Coordinating agency
d. Ensure coordination of technical data (collection, analysis, storage, and dissemination).	DHS and coordinating agency	Coordinating agency
e. Ensure Federal protective action recommendations are developed and provide advice and assistance to State, local, and tribal governments.	DHS and coordinating agency	Coordinating agency
f. Coordinate release of Federal information to the public.	DHS	Coordinating agency
g. Coordinate release of Federal information to Congress.	DHS	Coordinating agency
h. Keep the White House informed on all aspects of an incident	DHS	Coordinating agency
i. Ensure coordination of demobilization of Federal assets.	DHS	Coordinating agency

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00242 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.183

Response Coordination

Federal Agency Coordination

Incidents of National Significance	DHS is responsible for the overall coordination of Incidents of National Significance using elements described in the NRP Base Plan concept of operations.
Other Radiological Incidents	▪ The agency with primary responsibility for coordinating the Federal response to a radiological incident serves as the coordinating agency. ▪ The coordinating agency coordinates the actions of Federal agencies related to the incident utilizing this annex, agency-specific plans, and/or the NCP, as appropriate. ▪ Cooperating agencies provide technical and resource support, as requested by the coordinating agency. ▪ The coordinating agency may establish a field facility; assist State, local, and tribal response organizations; monitor and support owner/operator activities (when there is an owner or operator); provide technical support to the owner/operator, if requested; and serve as the principal Federal source of information about incident conditions.

Coordinating Radiological Aspects of an Incident

Incidents of National Significance	▪ DHS and the coordinating agency coordinate Federal activities related to responding to and recovering from the radiological aspects of an incident. They are assisted by cooperating agencies, as requested. ▪ The coordinating agency provides a hazard assessment of conditions that might have significant impact and ensures that measures are taken to mitigate the potential consequences.
Other Radiological Incidents	The coordinating agency coordinates Federal activities related to response and recovery of the radiological aspects of an incident, assisted by cooperating agencies, as requested.

Incident Security Coordination

Incidents of National Significance	DHS and the coordinating agency are responsible for coordinating security activities related to Federal response operations.
Other Radiological Incidents	The coordinating agency coordinates security activities related to Federal response operations.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00243 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.184

Incident Security Coordination (Continued)

Incidents of National Significance and Other Radiological Incidents	▪ DOD, DOE, or NASA, as the appropriate coordinating agency, may establish NDAs or NSAs to safeguard classified information and/or restricted data, or equipment and material, and place non-Federal lands under Federal control for the duration of the incident. DOD, DOE, or NASA, as appropriate, coordinates security in and around these locations, as necessary. ▪ For incidents at other Federal or private facilities, the owner/operator provides security within the facility boundaries. If a release of radioactive material occurs beyond the facility boundaries, State, local, or tribal governments provide security for the release area. ▪ State, local, and tribal governments provide security for radiological incidents occurring on public lands (e.g., a transportation incident). ▪ If needed, ESF #13 – Public Safety and Security may be activated to provide supplemental security resources and capabilities.

Technical Data Management

Incidents of National Significance	▪ DHS and the coordinating agency approve the release of all data to State, local, and tribal governments. ▪ For incidents involving terrorism, the coordinating agency consults with other members of the JFO Coordination Group as issues arise regarding the sharing of sensitive information that may be needed, on a need-to-know basis, for responder and public safety. ▪ DHS and the coordinating agency, in consultation with the JFO Coordination Group and State, local, and tribal governments, determine if the severity of an incident warrants a request for Nuclear Incident Response Team (NIRT) assets. ▪ The IMAAC is responsible for production, coordination, and dissemination of consequence predictions for an airborne hazardous material release. The IMAAC generates the single Federal prediction of atmospheric dispersions and their consequences utilizing the best available resources from the Federal Government.
Other Radiological Incidents	The coordinating agency authorizes the release of all data to State, local, and tribal governments.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00244 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.185

Technical Data Management (Continued)

Incidents of National Significance and Other Radiological Incidents	▪ The coordinating agency oversees the collection, analysis, storage, and dissemination of all technical data through the entire process. ▪ The coordinating agency is responsible for ensuring the sharing of all technical data, including outputs from the FRMAC, the Advisory Team, and the IMAAC, with all appropriate response organizations. ▪ Federal monitoring and assessment activities are coordinated with State, local, and tribal governments. Federal agency plans and procedures for implementing this activity are designed to be compatible with the radiological emergency planning requirements for State and local governments, specific facilities, and existing memorandums of understanding and interagency agreements. ▪ Prior to the on-scene arrival of the coordinating agency, Federal first responders may provide radiological monitoring and assessment data to State, local, and tribal governments as requested in support of protective action decisionmaking. Federal first responders also begin collecting data for transmission to the coordinating agency. If a FRMAC is established, the coordinating agency provides a mechanism for transmitting data to and from the FRMAC. Prior to the initiation of FRMAC operations, Federal first responders coordinate radiological monitoring and assessment data with the DOE Consequence Management Home Team (CMHT) or the Consequence Management Response Team (CMRT). (Note: A CMHT provides a reach-back capability to support the CMRT. The CMRT functions as an advance element of the FRMAC to establish contact with on-scene responders to coordinate Federal radiological monitoring and assessment activities.) ▪ DOE and other participating Federal agencies learn of an emergency when they are alerted to a possible problem or receive a request for radiological assistance. DOE maintains national and regional coordination offices as points of access to Federal radiological emergency assistance. Requests for Radiological Assessment Program (RAP) teams are generally directed to the appropriate DOE Regional Coordinating Office. All other requests for Federal radiological monitoring and assessment go directly to DOE's Emergency Operations Center (EOC) in Washington, DC. When other agencies receive requests for Federal radiological monitoring and assessment assistance, they notify the DOE EOC.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00245 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.186

Technical Data Management (Continued)

Incidents of National Significance and Other Radiological Incidents (Continued)	▪ DOE may respond to a State or coordinating agency request for assistance by dispatching a RAP team. If the situation requires more assistance than a RAP team can provide, DOE alerts or activates additional resources. These resources can include the establishment of a FRMAC as the coordination center for Federal radiological assessment activities. DOE may respond with additional resources including the Aerial Measurement System (AMS) to provide wide-area radiation monitoring, Radiation Emergency Assistance Center/Training Site (REAC/TS) medical advisory teams, National Atmospheric Release Advisory Center (NARAC) support, or if the accident involves a U.S. nuclear weapon, the Accident Response Group (ARG). Federal and State agencies are encouraged to collocate their radiological assessment activities. Some participating Federal agencies have radiological planning and emergency responsibilities as part of their statutory authority, as well as established working relationships with State counterpart agencies. The monitoring and assessment activity, coordinated by DOE, does not alter these responsibilities but complements them by providing for coordination of the initial Federal radiological monitoring and assessment response activity. ▪ Responsibility for coordinating radiological monitoring and assessment activities may transition to EPA at a mutually agreeable time, and after consultation with State, local, and tribal governments, the coordinating agency, and the JFO Coordination Group.

Protective Action Recommendations

Incidents of National Significance	DHS and the coordinating agency oversee the development of Federal Protective Action Recommendations and provide advice and assistance to State, tribal, and local governments. Federal Protective Action Recommendations are developed by the Advisory Team, in conjunction with the coordinating agency. Federal Protective Action Recommendations may include advice and assistance on measures to avoid or reduce exposure of the public to radiation from a release of radioactive material. This includes advice on emergency actions such as sheltering, evacuation, and prophylactic use of potassium iodide. It also includes advice on long-term measures, such as restriction of food, temporary relocation, or permanent resettlement, to avoid or minimize exposure to residual radiation or exposure through the ingestion pathway.
Other Radiological Incidents	The coordinating agency, in consultation with the Advisory Team, develops and provides Protective Action Recommendations.
Incidents of National Significance and Other Radiological Incidents	State, local, and tribal governments are responsible for implementing protective actions as they deem appropriate.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00246 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.187

Public Information Coordination

Incidents of National Significance and Other Radiological Incidents	DHS, in consultation with other agencies and the JFO Coordination Group oversees and manages the establishment of a Joint Information Center (JIC), if required.
Other Radiological Incidents	The coordinating agency may establish a JIC depending on the needs of the incident response.
Incidents of National Significance and Other Radiological Incidents	▪ Owners/operators and Federal, State, local, tribal, and other relevant information sources coordinate public information to the extent practical with the JIC. Communication with the public is accomplished in accordance with procedures outlined in the ESF #15 – External Affairs Annex and the Public Affairs Support Annex. ▪ It may be necessary to release Federal information regarding public health and safety. In this instance, Federal agencies coordinate with the coordinating agency and State, local, and tribal governments in advance, or as soon as possible after the information is released.

Congressional Coordination

Incidents of National Significance	DHS coordinates Federal responses to congressional requests for information. Points of contact for this function are the congressional liaison officers. All Federal agency congressional liaison officers and congressional staffs seeking site-specific information about an incident should contact the DHS Office of Legislative Affairs and the coordinating agency. While Congress may request information directly from any Federal agency, any agency responding to such requests shall inform DHS and the coordinating agency.
Other Radiological Incidents	The coordinating agency is responsible for congressional coordination, consulting with DHS as required.

White House Coordination

Incidents of National Significance	DHS submits reports to the President and keeps the White House informed of all aspects of the incident. While the White House may request information directly from any Federal agency, any agency responding to such requests must promptly inform DHS and the coordinating agency.
Other Radiological Incidents	The coordinating agency is responsible for any necessary White House coordination, consulting with DHS as requested. Note that these actions can take place during the transition from response to recovery.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00247 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.188

Deactivation/Demobilization Coordination

Incidents of National Significance	DHS and the coordinating agency, in consultation with the JFO Coordination Group and State, local, and tribal governments, develop plans to demobilize the Federal presence.
Other Radiological Incidents	The coordinating agency discontinues incident operations when a centralized Federal coordination presence is no longer required, or when its statutory responsibilities are fulfilled. Prior to discontinuing operations, the coordinating agency coordinates this decision with each Federal agency and State, local, and tribal governments.

International Coordination

Incidents of National Significance and Other Radiological Incidents	▪ In the event of an actual or potential environmental impact upon the United States or its possessions, territories, or territorial waters from a radiological emergency originating on foreign soil or, conversely, a domestic incident with an actual or potential foreign impact, DHS and the coordinating agency immediately inform the Department of State (DOS), which is responsible for official interactions with foreign governments. In either case (foreign incident with domestic impact, or vice versa), the coordinating agency consults with DHS, and DHS makes a determination on whether it is an Incident of National Significance. DHS and the coordinating agency keep DOS informed of all Federal incident management activities. ▪ DOS coordinates notification and information-gathering activities with foreign governments, except in cases where existing bilateral agreements permit direct communication. Where the coordinating agency has existing bilateral agreements that permit direct exchange of information, the coordinating agency keeps DOS informed of consultations with their foreign counterparts. DHS and the coordinating agency ensure that any offers of assistance to, or requests from, foreign governments are coordinated with DOS. ▪ The National Oceanic and Atmospheric Administration is the point of interaction with the hydrometeorological services of other countries. International response activities are accomplished in accordance with the International Coordination Support Annex.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00248 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.189

Victim Decontamination/Population Monitoring

Incidents of National Significance and Other Radiological Incidents	▪ External monitoring and decontamination of possibly affected victims are accomplished locally and are the responsibility of State, local, and tribal governments. Federal resources are provided at the request of, and in support of, the affected State(s). HHS, through ESF #8 and in consultation with the coordinating agency, coordinates Federal support for external monitoring of people and decontamination. ▪ HHS assists and supports State, local, and tribal governments in performing monitoring for internal contamination and administering available pharmaceuticals for internal decontamination, as deemed necessary by State health officials. ▪ HHS assists local and State health departments in establishing a registry of potentially exposed individuals, perform dose reconstruction, and conduct long-term monitoring of this population for potential long-term health effects.

Other Federal Resource Support

For Stafford Act or Federal-to-Federal support incidents, DHS/EPR/FEMA coordinates the provision of Federal resources and assistance to affected State, local, and tribal governments as part of the JFO Operations Section or other appropriate location established by DHS/EPR/FEMA.

Recovery

- For an Incident of National Significance, DHS coordinates overall Federal recovery activities, while the coordinating agency maintains responsibility for managing the Federal technical radiological cleanup activities in accordance with NRP mechanisms.
- For all radiological incidents, the coordinating agency coordinates environmental remediation/cleanup in concert with cognizant State, local, and tribal governments, and owners/operators, as applicable. While retaining overall technical lead, a coordinating agency may require support from a cooperating agency that has significant cleanup/recovery experience and capabilities (e.g., EPA, U.S. Army Corps of Engineers (USACE)) for a long-term cleanup. The initial coordinating agency may request that the coordinating agency role be transitioned to a cooperating agency to manage long-term cleanup efforts.
- State, local, and tribal governments primarily are responsible for planning the recovery of the affected area (the term "recovery," as used here, encompasses any action dedicated to the continued protection of the public and resumption of normal activities in the affected area). Recovery planning is initiated at the request of the State, local, or tribal governments, and generally does not take place until the initiating conditions of the incident have stabilized and immediate actions to protect public health, safety, and property are accomplished. Upon request, the Federal government assists State, local, and tribal governments develop and execute recovery plans.
- Private owners/operators have primary responsibility for recovery planning activities and eventual cleanup within their facility boundaries and may have responsibilities for recovery activities outside their facility under applicable legal obligations (e.g., contractual, licensee, CERCLA).
- The DOE FRMAC Director works closely with the Senior EPA representative to facilitate a smooth transition of the Federal radiological monitoring and assessment coordination responsibility to EPA at a mutually agreeable time, and after consultation with DHS, the JFO Coordination Group, and State, local, and tribal

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00249 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.190

governments. The following conditions are intended to be met prior to transfer:

- The immediate emergency condition is stabilized;
- Offsite releases of radioactive material have ceased, and there is little or no potential for further unintentional offsite releases;
- The offsite radiological conditions are characterized and the immediate consequences are assessed;
- An initial long-range monitoring plan has been developed in conjunction with the affected State, local, and tribal governments and appropriate Federal agencies; and
- EPA has received adequate assurances from the other Federal agencies that they are committing the required resources, personnel, and funds for the duration of the Federal response.

- Radiological monitoring and assessment activities are normally terminated when DHS, in consultation with the coordinating agency, other participating agencies, and State, local, and tribal governments, determines that:
  - There is no longer a threat to public health and safety or the environment;
  - State, local, and tribal resources are adequate for the situation; and
  - There is mutual agreement among the agencies involved to terminate monitoring and assessment.

Federal Assets Available Upon Request by the Coordinating Agency or DHS

Federal Radiological Monitoring and Assessment Center

DOE is responsible for developing and maintaining FRMAC policies and procedures, determining FRMAC composition, and maintaining FRMAC operational readiness. The FRMAC is established at or near the incident location in coordination with DHS, the coordinating agency, other Federal agencies, and State, local, and tribal authorities. A FRMAC normally includes representation from DOE, EPA, the Department of Commerce, the National Communications System (DHS/IAIP/NCS), USACE, and other Federal agencies as needed. Regardless of who is designated as the coordinating agency, DOE, through the FRMAC or DOE CMHT and CMRT, coordinates radiological monitoring and assessment activities for the initial phases of the response. When the FRMAC is transferred to the EPA, they assume responsibility for coordination of radiological monitoring and assessment activities.

Advisory Team for Environment, Food, and Health

- The Advisory Team includes representatives from DHS, EPA, the Department of Agriculture (USDA), the Food and Drug Administration, the Centers for Disease Control and Prevention, and other Federal agencies. The Advisory Team develops coordinated advice and recommendations for DHS, the JFO Coordination Group, the coordinating agency, and State, local, and tribal governments concerning environmental, food health, and animal health matters.
- The Advisory Team selects a chair for the Team.
- The Advisory Team provides recommendations in matters related to the following:
  - Environmental assessments (field monitoring) required for developing recommendations with advice from State, local, and tribal governments and/or the FRMAC senior Monitoring Manager;
  - Protective Action Guides and their application to the emergency;
  - Protective Action Recommendations using data and assessment from the FRMAC;
  - Protective actions to prevent or minimize contamination of milk, food, and water, and to prevent or minimize exposure through ingestion;

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00250 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.191

- Recommendations regarding the disposition of contaminated livestock, poultry, and contaminated foods, especially perishable commodities (e.g., meat in processing plants);
- Recommendations for minimizing losses of agricultural resources from radiation effects;
- Availability of food, animal feed, and water supply inspection programs to assure wholesomeness;
- Relocation, reentry, and other radiation protection measures prior to recovery;
- Recommendations for recovery, return, and cleanup issues;
- Health and safety advice or information for the public and for workers;
- Estimated effects of radioactive releases on human health and the environment; and
- Other matters, as requested by the coordinating agency.

DOE Radiological Assistance Program, Emergency Management Teams, and Nuclear Incident Response Team Assets

- RAP teams are located at DOE operations offices, national laboratories, and some area offices. They can be dispatched to a radiological incident by the DOE regional coordinating offices responding to a radiological incident.

Additional DOE planning and response teams and capabilities are located at various DOE facilities throughout the country and can be dispatched, as needed, to a radiological incident.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00251 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.192

Responsibilities

American Red Cross	(See the ESF #6 – Mass Care, Housing, and Human Services Annex for additional information.) Assesses the mass care consequences of a radiological incident, and in conjunction with State, local, and tribal (including private-sector) mass care organizations, develop and implement a sustainable short-term and long-term strategy for effectively addressing the consequences of the incident.
Department of Agriculture	(See the ESF #11 – Agriculture and Natural Resources Annex for additional information.) ▪ Inspects meat and meat products, poultry and poultry products, and egg products identified for interstate and foreign commerce to ensure that they are safe for human consumption. ▪ Assists, in conjunction with HHS, in monitoring the production, processing, storage, and distribution of food through the wholesale level to eliminate contaminated product or to reduce the contamination in the product to a safe level. ▪ Collects agricultural samples within the Ingestion Exposure Pathway Emergency Planning Zone (through the FRMAC). Assists in the evaluation and assessment of data to determine the impact of the incident on agriculture. ▪ Assesses damage to crops, soil, livestock, poultry, and processing facilities and incorporates findings in a damage assessment report. ▪ Provides emergency communications assistance to the agricultural community through the State Research, Education, and Extension Services electronic mail, or other USDA telecommunications systems. ▪ Supports/advises on decontamination and screening of pets and farm animals that may be exposed to radioactive material. ▪ Assists in animal carcass disposal.
Department of Commerce	▪ Provides operational weather observations and prepares forecasts tailored to support emergency incident management activities. ▪ Provides plume dispersion assessment and forecasts to the IMAAC and/or coordinating agency, in accordance with established procedures. ▪ Archives, as a special collection, the meteorological data from national observing and numerical weather analysis and prediction systems applicable to the monitoring and assessment of the response. ▪ Ensures that marine fishery products available to the public are not contaminated. ▪ Provides assistance and reference material for calibrating radiological instruments. ▪ Provides radiation shielding materials. ▪ In the event of materials potentially crossing international boundaries, serves as the agent for informing international hydrometeorological services and associated agencies through the mechanisms afforded by the World Meteorological Organization. ▪ Provides radioanalytical measurement support and instrumentation.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00252 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.193

Department of Defense	▪ Serves as a coordinating agency, as identified in Table 1, coordinating Federal actions for radiological incidents involving DOD facilities, including U.S. nuclear-powered ships, or material otherwise under their jurisdiction (e.g., transportation of material shipped by or for DOD). ▪ Provides Defense Support of Civil Authorities (DSCA) in response to requests for assistance during domestic incidents. With the exception for support provided under Immediate Response Authority, the obligation of DOD resources to support requests for assistance is subject to the approval of the Secretary of Defense. Details regarding DSCA are provided in the NRP Base Plan. ▪ Provides Immediate Response Authority under imminently serious conditions resulting from any civil emergency that may require immediate action to save lives, prevent human suffering, or mitigate great property damage. When such conditions exist and time does not permit prior approval from higher headquarters, local military commanders and responsible officials from DOD components and agencies are authorized by DOD directive, subject to any supplemental direction that may be provided by their DOD component, to take necessary action to respond to requests of civil authorities. All such necessary action is referred to as "Immediate Response."

Department of Defense/U.S. Army Corps of Engineers	(See the ESF #3 – Public Works and Engineering Annex for additional information.)
	▪ Directs response/recovery actions as they relate to ESF #3 functions, including contaminated debris management.
	▪ For RDD/IND incidents, provides response and cleanup support as a cooperating agency.
	▪ Integrates and coordinates with other agencies, as requested, to perform any or all of the following:
	  ▪ Radiological survey functions;
	  ▪ Gross decontamination;
	  ▪ Site characterization;
	  ▪ Contaminated water management; and
	  ▪ Site remediation.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00253 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.194

Department of Energy	▪ Serves as a coordinating agency, as identified in Table 1, coordinating Federal actions for radiological incidents involving DOE facilities or material otherwise under their jurisdiction (e.g., transportation of material shipped by or for DOE). ▪ Coordinates Federal offsite radiological environmental monitoring and assessment activities as lead technical organization in FRMAC (emergency phase), regardless of who is designated the coordinating agency. ▪ Maintains technical liaison with State and local agencies with monitoring and assessment responsibilities. ▪ Maintains a common set of all offsite radiological monitoring data in an accountable, secure, and retrievable form and ensures the technical integrity of FRMAC data. ▪ Provides monitoring data and interpretations, including exposure rate contours, dose projections, and any other requested radiological assessments, to the coordinating agency and to the States. ▪ Provides, in cooperation with other Federal agencies, the personnel and equipment to perform radiological monitoring and assessment activities, and provides on-scene analytical capability supporting assessments. ▪ Requests supplemental assistance and technical support from other Federal agencies as needed. ▪ Arranges consultation and support services through appropriate Federal agencies to all other entities (e.g., private contractors) with radiological monitoring functions and capabilities and technical and medical expertise for handling radiological contamination and population monitoring. ▪ Works closely with the Senior EPA representative to facilitate a smooth transition of the Federal radiological monitoring and assessment coordination responsibility to EPA at a mutually agreeable time and after consultation with the States and coordinating agency. ▪ Provides, in cooperation with other Federal and State agencies, personnel and equipment, including portal monitors, to support initial external screening and provides advice and assistance to State and local personnel conducting screening/decontamination of persons leaving a contaminated zone. ▪ Provides plume trajectories and deposition projections for emergency response planning assessments including source term estimates where limited or no information is available, including INDs and RDDs, to the IMAAC and/or coordinating agency, in accordance with established procedures. ▪ Upgrades, maintains, coordinates, and publishes documentation needed for the administration, implementation, operation, and standardization of the FRMAC. ▪ Maintains and improves the ability to provide wide-area radiation monitoring now resident in the AMS. ▪ Maintains and improves the ability to provide medical assistance, advisory teams, and training related to nuclear/radiological accidents and incidents now resident in the REAC/TS.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00254 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.195

Department of Energy (Continued)	▪ Maintains and improves the ability to provide near-real time assessments of the consequences of accidental or potential radiation releases by modeling the movement of hazardous plumes, and to correct modeled results through integration of actual radiation measurements obtained from both airborne and ground sources, resident in the NARAC. The NARAC also maintains and improves their ability to model the direct results (blast, thermal, radiation, EMP) of a nuclear detonation. ▪ Maintains and improves the first-response ability to assess an emergency situation and to advise decisionmakers on what further steps can be taken to evaluate and minimize the hazards of a radiological emergency resident in the RAP. ▪ Maintains and improves the ability to respond to an emergency involving U.S. nuclear weapons resident in the ARG. ▪ Maintains and improves the ability of the Consequence Management Planning Team, CMHT, and CMRTs to provide initial planning, coordination, and data collection and assessment prior to or in lieu of establishment of a FRMAC. ▪ Maintains and improves the ability of the Nuclear/Radiological Advisory Team to provide advice and limited technical assistance, including search, diagnostics, and effects prediction, as part of a Domestic Emergency Support Team. ▪ Maintains and improves the ability of the Search Response Teams to provide covert search capability using local support for initial nuclear search activities. ▪ Maintains and improves the ability of the Joint Technical Operations Team to provide technical operations advisory support and advanced technical assistance to the Federal primary or coordinating agency, provide extended technical support to other deployed operations through an emergency response home team; perform nuclear safety reviews to determine safe-to-ship status before moving a weapon of mass destruction (WMD) to an appropriate disposal location; and accept custody of nuclear or radiological WMD on behalf of DOE and provide for the final disposition of these devices. ▪ Maintains and improves the ability of Radiological Triage to determine through remote analysis of nuclear spectra collected on-scene if a radioactive object contains special nuclear materials. ▪ Assigns a Senior Energy Official (SEO) for any response involving the deployment of the DOE/NNSA emergency response assets. The SEO is responsible for the coordination and employment of these assets at the scene of a radiological event, and the deployed assets will work in support of and under the direction of the SEO.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00255 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.196

Department of Health and Human Services	(See the ESF #8 – Public Health and Medical Services Annex for additional information.) ▪ In conjunction with USDA, inspects production, processing, storage, and distribution facilities for human food and animal feeds that may be used in interstate commerce to ensure protection of the public health. ▪ Collects samples of agricultural products to monitor and assess the extent of contamination as a basis for recommending or implementing protective actions (through the FRMAC). ▪ Provides advice on proper medical treatment of the general population and response workers exposed to or contaminated by radioactive materials. ▪ Provides available medical countermeasures through deployment of the Strategic National Stockpile. ▪ Provides assessment and treatment teams for those exposed to or contaminated by radiation. ▪ Provides advice and guidance in assessing the impact of the effects of radiological incidents on the health of persons in the affected area. ▪ Manages long-term public monitoring and supports follow-on personal data collection, collecting and processing of blood samples and bodily fluids/matter samples, and advice concerning medical assessment and triage of victims. Tracks victim treatment and long-term health effects.
Department of Homeland Security/Emergency Preparedness and Response/Federal Emergency Management Agency	▪ Serves as the annex coordinator for this annex. ▪ In consultation with the coordinating agency, coordinates the provision of Federal resources and assistance to affected State, local, and tribal governments under the Stafford Act or Federal-to-Federal support provisions of the NRP. ▪ Monitors the status of the Federal response to requests for assistance from the affected State(s) and provides this information to the State(s). ▪ Keeps the coordinating agency informed of requests for assistance from the State(s) and the status of the Federal response. ▪ Identifies and informs Federal agencies of actual or apparent omissions, redundancies, or conflicts in response activity. ▪ Establishes and maintains a source of integrated, coordinated information about the status of all nonradiological resource support activities. ▪ Provides other support to Federal agencies responding to the emergency.
Department of Homeland Security/National Communications System	(See the ESF #2 – Communications Annex for additional information.) Acting through its operational element, the National Coordinating Center for Telecommunications (NCC), the NCS ensures the provision of adequate telecommunications support to Federal radiological incident response operations.
Department of Homeland Security/Science and Technology	(See the Science and Technology Support Annex for additional information.) Provides coordination of Federal science and technology resources as described in the Science and Technology Support Annex. This includes organization of Federal S&T support as well as assessment and consultation in the form of Scientific and Technical Advisory and Response Teams (STARTs) and the IMAAC.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00256 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC
46051.197

Department of Homeland Security/Customs and Border Protection (DHS/CBP)	▪ For incidents at the border, maintains radiation detection equipment and nonintrusive inspection technology at ports of entry and Border Patrol checkpoints to detect the presence of radiological substances transported by persons, cargo, mail, or conveyance arriving from foreign countries. ▪ Through its National Targeting Center, provides extensive analytical and targeting capabilities to identify and interdict terrorists and WMD. ▪ The CBP Weapons of Mass Destruction Teleforensic Center provides 24/7 support to DHS/CBP and other Federal law enforcement personnel in the identification of suspect hazardous material. ▪ The CBP Laboratory and Scientific Services staffs WMD Response Teams in strategic locations nationwide. ▪ Through the Container Security Initiative, DHS/CBP personnel are stationed at major foreign seaports in order to detect and prevent the transport of WMD on container vessels destined to the U.S. ▪ Has extensive authority and expertise regarding the entry, inspection, and admissibility of persons, cargo, mail, and conveyances arriving from foreign countries.

Department of Homeland Security/U.S. Coast Guard	▪ Serves as coordinating agency for incidents that occur in certain areas of the coastal zone, as identified in Table 1.
	▪ "Certain areas of the coastal zone," for the purposes of this document, means the following areas of the coastal zone as defined by the NCP:
	  ▪ Vessels, as defined in 33 CFR 160;
	  ▪ Areas seaward of the shoreline to the outer edge of the Economic Exclusion Zone; and
	  ▪ Within the boundaries of the following waterfront facilities subject to the jurisdiction of DHS/USCG; those regulated by 33 CFR 126 (Dangerous cargo handling), 127 (LPG/LNG), 128 (Passenger terminals), 140 (Outer Continental Shelf Activities), 1541-56 (Waterfront portions of Oil & Hazmat bulk transfer facilities – delineated as per the NCP), 105 (Maritime security - facilities).
	EPA is the coordinating agency for responses in areas of the coastal zone other than those defined above as certain areas of the coastal zone.
	▪ For incidents that have cross-boundary impacts, works with the other affected agency to determine how best to cooperatively respond consistent with the NCP model.
	▪ Serves as the coordinating agency for these incidents only during the prevention and emergency response phase, and transfers responsibility for later response phases to the appropriate agency, consistent with the NCP.
	▪ Because of its unique maritime jurisdiction and capabilities, is prepared to provide appropriate security, command and control, transportation, and support to other agencies that need to operate in the maritime domain.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00257 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.198

Department of Housing and Urban Development	▪ Reviews and reports on available housing for disaster victims and displaced persons. ▪ Assists in planning for and placing homeless victims in available housing ▪ Provides staff to support emergency housing within available resources. ▪ Provides housing assistance and advisory personnel.
Department of the Interior (DOI)	▪ Advises and assists in evaluating processes affecting radioisotopes in soils, including personnel, equipment, and laboratory support. ▪ Advises and assists in the development of geographic information systems databases to be used in the analysis and assessment of contaminated areas, including personnel and equipment. ▪ Advises and assists in assessing and dealing with impacts to natural resources, including fish and wildlife, subsistence uses, public lands, Indian tribal lands, land reclamation, mining, minerals, and water resources. Further guidance is provided in the Tribal Relations Support Annex and the ESF #11 – Agriculture and Natural Resources Annex. ▪ Provides liaison between federally recognized tribal governments and Federal, State, and local agencies for coordination of response activities. Additionally, DOI advises and assists DHS on economic, social, and political matters in the U.S. insular areas should a radiological incident occur in these areas.
Department of Justice/Federal Bureau of Investigation	Coordinates all law enforcement and criminal investigative response to acts of terrorism, to include intelligence gathering, hostage negotiations, and tactical operations. Further details regarding the FBI response are outlined in the Terrorism Incident Law Enforcement and Investigation Annex.
Department of Labor/Occupational Safety and Health Administration	Provides advice and technical assistance to DHS, the coordinating agency, and State, local, and tribal governments concerning the health and safety of response workers implementing the policies and concepts in this annex.
Department of State	▪ Coordinates foreign information-gathering activities and all contacts with foreign governments, except in cases where existing bilateral agreements permit direct agency-to-agency cooperation. ▪ Conveys the U.S. Government response to foreign offers of assistance.
Department of Transportation	(See the ESF #1 – Transportation Annex for further information.) Provides technical advice and assistance on the transportation of radiological materials and the impact of the incident on the transportation infrastructure.
Department of Veterans Affairs	▪ Provides medical assistance using the Medical Emergency Radiological Response Team. ▪ Provides temporary housing.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00258 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.199

Environmental Protection Agency	(See the Hazardous Materials Incident Annex for additional information.) ▪ Serves as a coordinating agency, as identified in Table 1. ▪ Provides resources, including personnel, equipment, and laboratory support (including mobile laboratories) to assist DOE in monitoring radioactivity levels in the environment. ▪ Assumes coordination of Federal radiological monitoring and assessment responsibilities after the transition from DOE. ▪ Assists in the development and implementation of a long-term monitoring plan and long-term recovery plan. ▪ Provides nationwide environmental monitoring data from the Environmental Radiation Ambient Monitoring Systems for assessing the national impact of the incident. ▪ Develops Protective Action Guides in coordination with the FRPCC. ▪ Recommends protective actions and other radiation protection measures. ▪ Recommends acceptable emergency levels of radioactivity and radiation in the environment. ▪ Prepares health and safety advice and information for the public. ▪ Estimates effects of radioactive releases on human health and the environment. ▪ Provides response and recovery actions to prevent, minimize, or mitigate a threat to public health, safety, or the environment caused by actual or potential releases of radioactive substances, including actions to detect, identify, contain, clean up, and dispose of such substances. ▪ Assists and supports the NIRT, when activated. ▪ Provides, in cooperation with other Federal agencies, the law enforcement personnel and equipment to conduct law enforcement operations and investigations for nuclear/radiological incidents involving criminal activity that are not terrorism related.
General Services Administration	(See the ESF #7 – Resource Support Annex for additional information.)
National Aeronautics and Space Administration	Serves as a coordinating agency, as identified in Table 1.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00259 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.200

Nuclear Regulatory Commission	▪ Serves as a coordinating agency, as identified in Table 1.
	▪ Provides technical assistance to include source term estimation, plume dispersion, and dose assessment calculations.
	▪ Provides assistance and recommendations concerning protective action measures as coordinating agency.
	▪ Provides assistance in Federal radiological monitoring and assessment activities.
	▪ For an incident at a facility licensed by the NRC or an Agreement State, or involving Atomic Energy Act licensed material:
	▪ The licensee takes action to mitigate the consequences of the incident and provides appropriate protective action recommendations to State, local, and tribal officials;
	▪ The NRC:
	  ▪ Performs an independent assessment of the incident and potential offsite consequences and, as appropriate, provides recommendations concerning any protective measures;
	  ▪ Performs oversight of the licensee, to include monitoring, evaluation of protective action recommendations, advice, assistance, and, as appropriate, direction; and
	  ▪ Dispatches, if appropriate, an NRC site team of technical experts to the licensee's facility.
	  ▪ Under certain situations involving the protection of public health/safety or national security, the NRC may take possession of special nuclear materials and/or operate certain facilities regulated by the NRC.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00260 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.201

ENCLOSURE C

3. Biological Incident Annex

46051.202

Biological Incident Annex

Coordinating Agency:

Department of Health and Human Services

Cooperating Agencies:

Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Homeland Security
Department of the Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of Veterans Affairs
U.S. Agency for International Development
Environmental Protection Agency
General Services Administration
U.S. Postal Service
American Red Cross

Introduction

Purpose

The purpose of the Biological Incident Annex is to outline the actions, roles, and responsibilities associated with response to a disease outbreak of known or unknown origin requiring Federal assistance. Actions described in this annex take place with or without a Presidential Stafford Act declaration or a public health emergency declaration by the Secretary of Health and Human Services (HHS). This annex applies only to Incidents of National Significance. This annex outlines biological incident response actions including threat assessment notification procedures, laboratory testing, joint investigative/response procedures, and activities related to recovery.

Scope

The broad objectives of the Federal Government's response to a biological terrorism event, pandemic influenza, emerging infectious disease, or novel pathogen outbreak are to:

- Detect the event through disease surveillance and environmental monitoring;
- Identify and protect the population(s) at risk;
- Determine the source of the outbreak;
- Quickly frame the public health and law enforcement implications;
- Control and contain any possible epidemic (including providing guidance to State and local public health authorities);
- Augment and surge public health and medical services;
- Track and defeat any potential resurgence or additional outbreaks; and
- Assess the extent of residual biological contamination and decontaminate as necessary.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00262 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.203

The unique attributes of this response require separate planning considerations that are tailored to specific health concerns and effects of the disease (e.g., terrorism versus natural outbreaks; communicable versus noncommunicable, etc.).

Specific operational guidelines, developed by the respective organizations to address the unique aspects of a particular disease or planning consideration, will supplement this annex and are intended as guidance to assist Federal, State, local, and tribal public health and medical planners.

Special Considerations

Detection of a bioterrorism act against the civilian population may occur in several different ways and involve several different modalities:

- An attack may be surreptitious, in which case the first evidence of dissemination of an agent may be the presentation of disease in humans or animals. This could manifest either in clinical case reports to domestic or international public health authorities or in unusual patterns of symptoms or encounters within domestic or international health surveillance systems.

- A terrorist-induced infectious disease outbreak initially may be indistinguishable from a naturally occurring outbreak; moreover, depending upon the particular agent and associated symptoms, several days could pass before public health and medical authorities even suspect that terrorism may be the cause. In such a case, criminal intent may not be apparent until some time after illnesses are recognized.

- Environmental surveillance systems, such as the BioWatch system, may detect the presence of a biological agent in the environment and trigger directed environmental sampling and intensified clinical surveillance to rule out or confirm an incident. If a case is confirmed, then these systems may allow for mobilization of a public health, medical, and law enforcement response in advance of the appearance of the first clinical cases or quick response after the first clinical cases are identified.

- The U.S. Postal Service may detect certain biological agents within the U.S. postal system. Detection of a biological agent in the mail stream triggers specific response protocols outlined in agency-specific standard operating procedures.

Policies

- This annex supports policies and procedures outlined in the ESF #8 – Public Health and Medical Services Annex, the ESF #10 – Oil and Hazardous Materials Response Annex, and the Terrorism Incident Law Enforcement and Investigation Annex.

- HHS serves as the Federal Government's primary agency for the public health and medical preparation and planning for and response to a biological terrorism attack or naturally occurring outbreak that results from either a known or novel pathogen, including an emerging infectious disease.

- State, local, and tribal governments are primarily responsible for detecting and responding to disease outbreaks and implementing measures to minimize the health, social, and economic consequences of such an outbreak.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00263 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.204

- If any agency becomes aware of an overt threat involving biological agents or indications that instances of disease may not be the result of natural causes, the Department of Justice must be notified through the Federal Bureau of Investigation (FBI)'s Weapons of Mass Destruction Operations Unit (WMDOU). The FBI, in turn, immediately notifies the Department of Homeland Security (DHS) Homeland Security Operations Center (HSOC) and the National Counterterrorism Center (NCTC). The Laboratory Response Network (LRN) is used to test samples for the presence of biological threat agents. Decisions on where to perform additional tests on samples are made by the FBI, in coordination with HHS. (See the Terrorism Incident Law Enforcement and Investigation Annex for additional information on the FBI's roles and responsibilities.)

- Once notified of a credible threat or natural disease outbreak, HHS convenes a meeting of ESF #8 partners to assess the situation and determine appropriate public health and medical actions. DHS coordinates overall nonmedical support and response actions across all Federal departments and agencies. HHS coordinates overall public health and medical emergency response efforts across all Federal departments and agencies.

- Consistent with ESF #8, DHS closely coordinates the National Disaster Medical System (NDMS) medical response with HHS. The FBI coordinates the investigation of criminal activities if such activities are suspected.

- HHS provides guidance to State and local authorities and collaborates closely with the FBI in the proper handling of any materials that may have evidentiary implications (e.g., LRN samples, etc.) associated with disease outbreaks suspected of being terrorist or criminal in nature.

- Other Federal departments and agencies may be called upon to support HHS during the various stages of a disease outbreak response in the preparation, planning, and/or response processes.

- If there is potential for environmental contamination, HHS collaborates with the Environmental Protection Agency (EPA) in developing sampling strategies and sharing results.

- Given the dynamic nature of a disease outbreak, HHS, in collaboration with other departments and agencies, determines the thresholds for a comprehensive Federal Government public health and medical response. These thresholds are based on specific event information rather than predetermined risk levels.

- Any Federal public announcement, statement, or press release related to a threat or actual bioterrorism event must be coordinated with the DHS Public Affairs Office.

Planning Assumptions

- In a large disease outbreak, Federal, State, local, and tribal officials require a highly coordinated response to public health and medical emergencies. The outbreak also may affect other countries and therefore involve extensive coordination with the Department of State (DOS).

- Disease transmission can occur via an environmental contact such as atmospheric dispersion, person-to-person contact, animal-to-person contact, insect vector-to-person contact, or by way of contaminated food or water.

- A biological incident may be distributed across multiple jurisdictions simultaneously, requiring a nontraditional incident management approach. This approach could require the simultaneous management of multiple "incident sites" from national and regional headquarters locations in coordination with multiple State and local jurisdictions.

- A response to noncontagious public health emergencies may require different planning assumptions or factors.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00264 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.205

- The introduction of biological agents, both natural and deliberate, are often first detected through clinical or hospital presentation. However, there are other methods of detection, including environmental surveillance technologies such as BioWatch and syndromic surveillance.
- No single entity possesses the authority, expertise, and resources to act unilaterally on the many complex issues that may arise in response to a disease outbreak and loss of containment affecting a multijurisdictional area. The national response requires close coordination with numerous agencies at all levels of government and the private sector.
- The Federal Government supports affected State, local, and tribal health jurisdictions as requested or required. The response by HHS and other Federal agencies is flexible and adapts as necessary as the outbreak evolves.
- The LRN provides for rapid public health assessment of the potential for human illness associated with exposure and the scope of this kind of risk. The LRN also addresses the need for law enforcement notification necessary to initiate threat assessment for criminal intent, and chain of custody procedures. Early HHS, FBI, and DHS coordination enhances the likelihood of successful preventative and investigative activities necessary to neutralize threats and attribute the source of the outbreak.
- Response to disease outbreaks suspected of being deliberate in origin requires consideration of special law enforcement and homeland security requirements.
- Test results from non-LRN facilities are considered a "first pass" or "screening" test (with the exception of the Legislative Branch, which has a separate lab system that is equivalent to LRN facilities).
- Any agency or organization that identifies an unusual or suspicious test result should contact the FBI to ensure coordination of appropriate testing at an HHS-certified LRN laboratory.
- HHS has identified specific Department of Defense laboratories that meet the standards and requirements for LRN membership.
- All threat and public health assessments are provided to the HSOC.

Concept of Operations

Biological Agent Response

The key elements of an effective biological response include (in nonsequential order):

- Rapid detection of the outbreak;
- Swift agent identification and confirmation;
- Identification of the population at risk;
- Determination of how the agent is transmitted, including an assessment of the efficiency of transmission;
- Determination of susceptibility of the pathogen to treatment;
- Definition of the public health, medical, and mental health implications;
- Control and containment of the epidemic;
- Decontamination of individuals, if necessary;
- Identification of the law enforcement implications/assessment of the threat;
- Augmentation and surging of local health and medical resources;
- Protection of the population through appropriate public health and medical actions;
- Dissemination of information to enlist public support;

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00265 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.206

- Assessment of environmental contamination and cleanup/decontamination of bioagents that persist in the environment; and
- Tracking and preventing secondary or additional disease outbreak.

Primary Federal functions include supporting State, local, and tribal public health and medical capacities according to the policies and procedures detailed in the NRP Base Plan and the ESF #8 Annex.

Suspicious Substances

Since there is no definitive/reliable field test for biological agents, all potential bioterrorism samples are transported to an LRN laboratory, where expert analysis is conducted using established HHS/Centers for Disease Control and Prevention (CDC) protocols/reagents. A major component of this process is to establish and maintain the law enforcement chain of custody and arrange for transport.

The following actions occur if a positive result is obtained by an LRN on an environmental sample submitted by the FBI or other designated law enforcement personnel:

- The LRN immediately notifies the local FBI of the positive test result;
- The FBI Field Office makes local notifications and contacts the FBI Headquarters WMDOU;
- FBI Headquarters convenes an initial conference call with the local FBI and HHS to review the results, assess the preliminary information and test results, and arrange for additional testing;
- FBI Headquarters immediately notifies DHS of the situation;
- Original samples may be sent to HHS/CDC for confirmation of LRN analyses;
- HHS provides guidance on protective measures such as prophylactic treatment and continued facility operation; and
- HHS and cooperating agencies support the determination of the contaminated area, decisions on whether to shelter in place or evacuate, and decontamination of people, facilities, and outdoor areas

Outbreak Detection

Determination of a Disease Outbreak

The initial indication of a major disease outbreak, intentional or naturally occurring, may be the recognition by public health and medical authorities that a significantly increased number of people are becoming ill and presenting to local healthcare providers. Therefore, the most critical decisionmaking support requires surveillance information, identification of the causative biological agent, a determination of whether the observations are or are not related to a naturally occurring outbreak, and the identification of the population(s) at risk.

Laboratory Confirmation

During the evaluation of a suspected disease outbreak, laboratory samples are distributed to appropriate laboratories. During a suspected terrorist event, sample information is provided to the FBI for investigative use and to public health and emergency response authorities for epidemiological use and agent characterization to facilitate and ensure timely public health and medical interventions. If the incident begins as an epidemic of unknown origin detected through Federal, State, local, or tribal health surveillance systems or networks, laboratory analysis is initiated through the routine public health laboratory network.

Identification (Analysis and Confirmation)

The samples being collected and the analyses being conducted must be sufficient to characterize the cause of the outbreak. LRN laboratories fulfill the Federal responsibility for rapid analysis of biological agents. In a suspected terrorism event, sample collection activities and testing are coordinated with FBI and LRN member(s).

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00266 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.207

Notification

Any disease outbreak suspected or identified by an agency within HHS or through another Federal public health partner is brought to the immediate attention of the HHS Assistant Secretary for Public Health Emergency Preparedness as detailed in the ESF #8 Annex or internal HHS policy documents, in addition to the notification requirements contained in the NRP Base Plan.

Following these initial notifications, the procedures detailed in the ESF #8 Annex are followed. Instances of disease that raise the "index of suspicion," as determined by HHS, are reported to FBI Headquarters. In these instances, FBI Headquarters, in conjunction with HHS, examines available law enforcement and intelligence information, as well as the technical characteristics and epidemiology of the disease, to determine if there is a possibility of criminal intent. If the FBI, in conjunction with HHS, determines that the information represents a potential credible terrorist threat, the FBI communicates the situation to the HSOC, which notifies the White House, as appropriate. If warranted, the FBI, HHS, and State, local, and tribal health officials conduct a joint law enforcement and epidemiological investigation to determine the cause of the disease outbreak, the extent of the threat to public health and public safety, and the individual(s) responsible.

Activation

Once notified of a threat or disease outbreak that requires or potentially requires significant Federal public health and/or medical assistance, HHS convenes a meeting of the ESF #8 organizations and HHS Operating Divisions (e.g., CDC, the Food and Drug Administration, etc.) to assess the situation and determine the appropriate public health and medical actions. DHS coordinates all nonmedical support, discussions, and response actions.

The immediate task following any notification is to identify the population affected and at risk and the geographic scope of the incident. The initial public health and medical response includes some or all of the following actions:

- Targeted epidemiological investigation (e.g., contact tracing);
- Intensified surveillance within healthcare settings for patients with certain clinical signs and symptoms;
- Intensified collection and review of potentially related information (e.g., contacts with nurse call lines, laboratory test orders, school absences, and over-the-counter pharmacy sales); and
- Organization of Federal public health and medical response assets (in conjunction with State, local, and tribal officials) to include personnel, medical supplies, and materiel (e.g., the Strategic National Stockpile (SNS)).

Actions

Controlling the Epidemic

The following steps are required to contain and control an epidemic affecting large populations:

- HHS assists State, local, and tribal public health and medical authorities with epidemic surveillance and coordination.
- HHS assesses the need for increased surveillance in States or localities not initially involved in the outbreak and notifies the appropriate State and local public health officials with surveillance recommendations should increased surveillance in these localities be needed.
- DHS coordinates with HHS and State, local, and tribal officials on the messages released to the public to ensure that communications are consistent and accurate. Messages should address anxieties, alleviate any unwarranted concerns or distress, and enlist cooperation with necessary control measures. Public health and medical messages to the public should be communicated by a recognized health authority (e.g., the Surgeon General). (See the Public Affairs Support Annex.)

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00267 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.208

- If the outbreak first arises within the United States, HHS, in coordination with DOS, immediately notifies and coordinates with appropriate international health agencies such as the World Health Organization (WHO) and Pan American Health Organization as needed. Given the nature of many disease outbreaks, this notification and coordination may have occurred earlier in the process according to internal operating procedures. HHS advises the HSOC when notifications are made to international health agencies.

- The public health system, starting at the local level, is required to initiate appropriate protective and responsive measures for the affected population, including first responders and other workers engaged. These measures include mass vaccination or prophylaxis for populations at risk and populations not already exposed, but who are at risk of exposure from secondary transmission or the environment. An overarching goal is to develop, as early as possible in the management of a bioterrorism incident, a dynamic, prioritized list of treatment recommendations based on epidemiologic risk assessment and the biology of the disease/ microorganism in question, linked to the deployment of the SNS and communicated to the general public.

- HHS evaluates the event with its partner organizations and makes recommendations to the appropriate public health and medical authorities regarding the need for quarantine, shelter-in-place, or isolation to prevent the spread of disease. HHS coordinates closely with DHS regarding recommendations for medical needs that are met by NDMS and the U.S. Public Health Service Commissioned Corps.

- The Governor of an affected State implements isolation and/or social-distancing requirements using State/local legal authorities. In order to prevent the interstate spread of disease, HHS may take appropriate Federal actions using the authorities granted by U.S.C. title 42, 42 CFR parts 70 and 71, and 21 CFR 1240. State, local, and tribal assistance with the implementation and enforcement of isolation and/or quarantine actions is utilized if Federal authorities are invoked.

- Where the source of the epidemic has been identified as originating outside the United States, whether the result of terrorism or a natural outbreak, HHS works in a coordinated effort with DHS/Border and Transportation Security/Customs and Border Protection (DHS/BTS/CBP) to identify and isolate persons, cargo, mail, or conveyances entering the United States that may be contaminated. HHS provides information and training, as appropriate, to DHS/BTS/CBP personnel on identifying the biological hazard and employing "first responder" isolation protocols.

- The scope of the outbreak may require mass isolation or quarantine of affected or potentially affected persons. Depending on the type of event, food, animals, and other agricultural products may need to be quarantined to prevent further spread of disease. In this instance HHS and, as appropriate, the Department of Agriculture work with State, local, and tribal health and legal authorities to recommend the most feasible, effective, and legally enforceable methods of isolation and quarantine.

Decontamination

For certain types of biological incidents (e.g., anthrax), it may be necessary to assess the extent of contamination and decontaminate victims, responders, animals, equipment, buildings, critical infrastructure (e.g., subways, water utilities), and large outdoor areas. Such decontamination and related activities take place consistent with the roles and responsibilities, resources and capabilities, and procedures contained in the ESF #8 and ESF #10 Annexes, the Terrorism Incident Law Enforcement and Investigation Annex, and the Catastrophic Incident Annex. (Note: Currently no decontamination chemicals are registered (under the Federal Insecticide, Fungicide, and Rodenticide Act) for use on biological agents, and responders must request an emergency exemption from the EPA before chemicals can be used for biological decontamination.)

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00268 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.209

Special Issues

International Notification

A biological incident may involve internationally prescribed reportable diseases. In addition to case reporting, epidemics of disease with global public health significance must also be reported to international public health authorities.

Once a positive determination is made of an epidemic involving a contagious biological agent, HHS notifies DOS and DHS. HHS, in coordination with DOS, notifies the WHO and other international health agencies as appropriate.

Allocation and Rationing

If critical resources for protecting human life are insufficient to meet all domestic needs, the Secretary of HHS makes recommendations to the Secretary of Homeland Security regarding the allocation of scarce Federal public health and medical resources.

Responsibilities

The procedures in this annex are built on the core coordinating structures of the NRP. The responsibilities of each department and agency are described in the respective ESFs and Incident Annexes.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00269 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.210

ENCLOSURE D

QUESTION 29

8/1/05 RESPONSE TO SENATOR LEAHY CONCERNING:

"Alerting Law Enforcement Officers to Terrorism Suspects Through VGTOF"

46051.211

U.S. Department of Justice

Federal Bureau of Investigation

Office of the Director

Washington, D.C. 20535

August 1, 2005

Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Leahy:

During the Senate Judiciary Committee's oversight hearing on July 27, 2005, you asked me to follow up on our discussion concerning the guidance provided to law enforcement officers when they encounter individuals who appear on a watchlist maintained by the Terrorist Screening Center. I appreciate this opportunity to respond to your request.

Attached is an explanation of the information provided to law enforcement officers when a check of the National Crime Information Center's database indicates that the subject has been entered in the Violent Gang and Terrorist Offender File (VGTOF). VGTOF provides the handling codes to which you referred during the hearing.

I appreciate your interest in this matter and your support for this and other FBI efforts. If you have additional questions, please do not hesitate to contact me.

Sincerely,

Robert S. Mueller, III
Director

Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Alerting Law Enforcement Officers to Terrorism Suspects Through VGTOF

When a law enforcement officer queries the National Crime Information Center (NCIC), several items of information may be obtained, including past offenses, sentences, and outstanding arrest warrants. This information may identify the person as armed and dangerous or may otherwise alert the officer to information important to the officer's safety.

The Violent Gang and Terrorist Organization File (VGTOF) is a component of NCIC. A subject is included in VGTOF if he or she is known or suspected to have engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (as provided in Homeland Security Presidential Directive (HSPD) 6 (9/16/03)) and certain identifying information is known to law enforcement officials, as discussed further below. Because all those associated with terrorism are potentially dangerous, all terrorism-related VGTOF entries are designated "Approach with Caution," regardless of whether the individual's terrorism-related activity has been violent. Unrelated to the individual threat that may be posed by a given VGTOF subject, all terrorism-related VGTOF entries receive one of four handling codes to reflect the nature and quality of the identifying information available on the subject and to identify the proper law enforcement response if the subject is encountered. As discussed further below, these codes are based on established criteria and are updated if warranted by new information. These handling codes are as follows.

Handling Code 1

Warning - Approach with Caution.

Arrest this individual. This individual is associated with terrorism. Once this individual is arrested, immediately contact the Terrorist Screening Center at (866) 872-9001 for additional information and direction.

If you are a Border Patrol Officer, immediately call the NTC [U.S. Customs and Border Protection's National Targeting Center].

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00272 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.213

Handling Code 2

Warning - Approach with Caution.

Please detain this individual for a reasonable amount of time for questioning. This individual is of investigative interest to law enforcement regarding association with terrorism. Immediately contact the Terrorist Screening Center at (866) 872-9001 for additional direction.

If you are a Border Patrol Officer, immediately contact the NTC.

Handling Code 3

Do Not Alert This Individual to This Notice.

The person queried through this search may be an individual identified by intelligence information as having possible ties with terrorism. Contact the Terrorist Screening Center at (866) 872-9001 for additional identifying information available to assist you in making this determination.

Do not arrest this individual unless there is evidence of a violation of federal, state, or local statutes. Conduct logical investigation using techniques authorized in your jurisdiction and ask probing questions to determine if this individual is identical to the person of law enforcement interest.

Warning - Approach with Caution.

If you are a Border Patrol Officer, immediately call the NTC.

Do Not Advise This Individual That They Are on a Terrorist Watchlist.

Handling Code 4

Do Not Alert This Individual to This Notice.

The person queried through this search may be an individual identified by intelligence information as having possible ties with

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00273 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.214

terrorism.

Contact the Terrorist Screening Center at (866) 872-9001 for additional identifying information that may be available to assist you in making this determination.

Do not arrest this individual unless there is evidence of a violation of federal, state, or local statutes. Attempt to obtain sufficient identification information to positively identify this individual in a manner consistent with the techniques authorized in your jurisdiction.

Warning - Approach with Caution.

If you are a Border Patrol Officer immediately call the NTC.

Do Not Advise This Individual That They Are on a Terrorist Watchlist.

All four handling codes indicate "Approach with Caution" because of the inherent danger in approaching a person known or suspected to have engaged in terrorist-related activity. The VGTOF handling code is not, however, designed to alert the law enforcement officer to the threat posed by the individual, since an individual's association with terrorism does not necessarily mean the individual is personally dangerous While other NCIC information may alert the officer to a history of violent crimes, the VGTOF handling code itself does not provide this information. The VGTOF handling code instead relates to the amount and nature of the information available about the individual and, as additional information is obtained, a handling code may be revised to reflect that fact. For example, on 6/16/05 several thousand records were changed from Handling Code 4 to Handling Code 3 because full dates of birth or passport numbers were obtained. This migration from Handling Code 4 to Code 3 was the routine result of TSC's quality assurance process.

It is also important to understand how these handling codes are assigned. As a threshold matter, handling codes are assigned only to those included in VGTOF (as noted above, placement in VGTOF requires satisfaction of the criteria established by HSPD-6). The assignment of a VGTOF handling code is based on the following specific criteria.

- Among other things, the assignment of Handling Code 1 requires that there be a current, valid United States warrant or indictment for the subject, or an international arrest warrant or Interpol warrant accompanied by a corresponding warrant issued in the United States (such as a warrant for Unlawful Flight to Avoid Prosecution)

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00274 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.215

- The assignment of Handling Code 2 requires a reasonable. articulable suspicion of criminal domestic or international terrorism activity, a commitment from the Department of Homeland Security that they will issue a "Detainer" should the individual be encountered by law enforcement, or the presence of exigent circumstances. The determination that such a basis exists must be reviewed for legal sufficiency by the "nominating" office's Chief Division Counsel and the Office of the General Counsel at FBI Headquarters.

- Handling Code 3 is assigned to a person who has been placed in VGTOF consistent with HSPD-6 criteria where the subject's record contains the full first name, full last name, and either a complete date of birth or an accurate passport number, but does not meet the threshold for the assignment of Handling Code 1 or 2.

- Like Handling Code 3, Handling Code 4 is assigned to a person who has been placed in VGTOF consistent with HSPD-6 criteria, but only the subject's full first name and full last name are known, without the benefit of a complete date of birth or passport number.

As is apparent from the above instructions to law enforcement officers, all four handling codes request TSC notification. The program originally provided for Code 4 notifications to TSC only if the circumstances of the encounter were consistent with terrorist activity, because TSC was concerned that it would be unable to assist officers due to the very limited amount of information available as to Code 4 individuals. TSC was particularly concerned that if a law enforcement officer were to contact TSC with respect to numerous Code 4 subjects and received no assistance, the officer would stop contacting TSC not only in Code 4 cases but in Code 1, 2, and 3 cases as well, depriving both the officer and the TSC of valuable information.

This policy was changed in June 2005, and NCIC was asked to revise the instructions provided in Code 4 cases to request the same TSC notification requested for Codes 1, 2, and 3. This change was made based on the desire to capture as much intelligence information as possible by trying to make a positive identity match for all those encountered. NCIC has made the requested change, and law enforcement officers are now asked to notify TSC when a Code 4 individual is encountered. The effectiveness of this revision will be evaluated by TSC and efforts will continue to ensure the information provided to law enforcement officers is as complete and helpful as possible.

7/29/05

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00275 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.216

ENCLOSURE E

QUESTION 40

5/24/05 LETTER TO SENATE SELECT COMMITTEE ON INTELLIGENCE

46051.217

U.S. Department of Justice

Office of Legislative Affairs

RECEIVED

2005 JUL -5 AM 11: 57

OIPR
DEPT OF JUSTICE

Office of the Assistant Attorney General

Washington, D.C. 20530

SECRET

MAY 24 2005

Senator Pat Roberts, Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Chairman Roberts:

I write to express the Department of Justice's strong opposition to any attempt to impose an "ascertainment" requirement on the implementation of multi-point or "roving" surveillance conducted under the Foreign Intelligence Surveillance Act (FISA). (U)

As the Members of this Committee are well aware, a roving surveillance order attaches to a particular target rather than to a particular phone or other communications facility. Since 1986, law enforcement has been able to use roving wiretaps to investigate ordinary crimes, including drug offenses and racketeering. Before the USA PATRIOT Act, however, FISA did not include a roving surveillance provision. Therefore, each time a suspect changed communication providers, investigators had to return to the FISA Court for a new order just to change the name of the facility to be monitored and the "specified person" needed to assist in monitoring the wiretap. However, international terrorists and spies are trained to thwart surveillance by regularly changing communication facilities, especially just prior to important meetings or communications. Therefore, without roving surveillance authority, investigators were often left two steps behind sophisticated terrorists and spies. (U)

Thankfully, section 206 of the USA PATRIOT Act ended this problem by providing national security investigators with the authority to obtain roving surveillance orders from the FISA Court. This provision has put investigators in a much better position to counter the actions of spies and terrorists who are trained to thwart

SECRET

Classified by: James A. Baker, Counsel for Intelligence Policy, Office of Intelligence Policy and Review, U.S. Department of Justice
Reason: 1.4(c)
Declassify on: X1

Declassified by James A. Baker
Counsel for Intelligence Policy
OIPR/USDOJ
Date: 7/9/05

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00277 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.218

surveillance. This is a tool that we do not use often, but when we use it, it is critical. As of March 30, 2005, it had been used 49 times and has proven effective in monitoring foreign powers and their agents. (U)

Some in Congress have expressed the view that an "ascertainment" requirement should be added to the provisions in FISA relating to "roving" surveillance authority. Section 2 of the S. 737, the Security and Freedom Ensured Act of 2005 ("SAFE Act"), for example, would provide that such surveillance may only be conducted when the presence of the target at a particular facility or place is "ascertained" by the person conducting the surveillance. (U)

Proponents of the SAFE Act have claimed that this provision would simply impose the same requirement on FISA "roving" surveillance orders that pertains to "roving" wiretap orders issued in criminal investigations, but this is wholly inaccurate. The relevant provision of the criminal wiretap statute states that the roving interception of oral communications "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." *See* 18 U.S.C. § 2518(12). With respect to the roving interception of wire or electronic communications, however, the criminal wiretap statute imposes a more lenient standard, providing that surveillance can be conducted "only for such time as it is reasonable to presume that [the target of the surveillance] is or was reasonably proximate to the instrument through which such communication will be or was transmitted." *See* 18 U.S.C. § 2518(11)(b)(iv). (U)

Any "ascertainment" requirement, however, whether it is the one contained in the SAFE Act or the one currently contained in the criminal wiretap statute, should not be added to FISA. Any such requirement would deprive national security investigators of necessary flexibility in conducting sensitive surveillance. Due to the different ways in which foreign intelligence surveillance and criminal law enforcement surveillance are conducted as well as the heightened sophistication of terrorists and spies in avoiding detection, provisions from the criminal law cannot simply be imported wholesale into FISA. (U)

Targets of FISA surveillance are often among the most well-trained and sophisticated terrorists and spies in the world. As a result, they generally engage in detailed and extensive counter-surveillance measures. Adding an ascertainment requirement to FISA therefore runs the risk of seriously jeopardizing the Department's ability to effectively conduct surveillance of these targets because, in attempting to comply with such a requirement, agents would run the risk of exposing themselves to sophisticated counter-surveillance efforts. (U)

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00278 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.219

SECRET

In addition, an ascertainment requirement is unnecessary in light of the manner in which FISA surveillance is conducted. As the Members of this Committee are no doubt aware, intercepted communications under FISA are often not subject to contemporaneous monitoring but rather are later translated and culled pursuant to court-ordered minimization procedures. These procedures adequately protect the privacy concerns that we believe the proposed ascertainment provisions are intended in part to address. (U)

While we understand the concern that conversations of innocent Americans might be intercepted through roving surveillance under FISA, the Department does not believe that an ascertainment requirement is an appropriate mechanism for addressing this concern. Rather, we believe that the current safeguards contained in FISA along with those procedures required by the FISA Court amply protect the privacy of law-abiding Americans. (U)

First, under section 206, the target of roving surveillance must be identified or described in the order of the FISA Court, and if the target of the surveillance is only described, such description must be sufficiently specific to allow the FISA Court to find probable cause to believe that the specified target is a foreign power or agent of a foreign power. As a result, section 206 is always connected to a particular target of surveillance. Roving surveillance follows a specified target from phone to phone and does not "rove" from target to target. (U)

Second, surveillance under section 206 also can be ordered only after the FISA Court makes a finding that the actions of the specified target may have the effect of thwarting the surveillance (by thwarting the identification of those persons necessary to assist with the implementation of surveillance). (U)

Additionally, all "roving" surveillance orders under FISA must include Court-approved minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons. These are usually in the form of standard minimization procedures applicable to certain categories of surveillance, but the procedures may be modified in particular circumstances. (U)

(b)(1)1.4c

SECRET

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00279 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.220

SECRET

(b)(1)1.4c

In sum, the Department believes that the safeguards set forth in this letter reflect the appropriate balance between ensuring the effective surveillance of sophisticated foreign powers and their agents and protecting the privacy of the American people. The Department strongly opposes any attempt to disturb this balance by adding an ascertainment requirement to the provisions of FISA relating to roving surveillance authority. (U)

We hope that this information will be useful to the Committee as it considers the reauthorization of those USA PATRIOT Act provisions scheduled to sunset at the end of this year. Please do not hesitate to contact me if you have additional questions or concerns about this issue. (U)

Sincerely,

William E. Moschella

William Moschella
Assistant Attorney General

SECRET

4

46051.221

SUBMISSIONS FOR THE RECORD

Office of the Inspector General
United States Department of Justice

Statement of Glenn A. Fine
Inspector General, U.S. Department of Justice

before the

Senate Committee on the Judiciary

concerning

Oversight of the Federal Bureau of Investigation

July 27, 2005

Statement of Glenn A. Fine
Inspector General, U.S. Department of Justice,
before the
Senate Committee on the Judiciary
concerning
Oversight of the Federal Bureau of Investigation
July 27, 2005

Mr. Chairman, Senator Leahy, and Members of the Committee on the Judiciary:

Thank you for inviting me to testify regarding the Office of the Inspector General's (OIG) oversight work in the Federal Bureau of Investigation (FBI). After the September 11, 2001, terrorist attacks, counterterrorism became the top priority of the FBI. As a result, the OIG has completed a series of reviews examining FBI programs and operations related to counterterrorism and national security issues.

These OIG reviews include reports on the FBI's foreign language translation program, the recruitment and training of FBI intelligence analysts, the FBI's information technology initiatives such as the Trilogy Project and its Virtual Case File effort, the FBI's management of the Terrorist Screening Center, intelligence information in the FBI's possession prior to the September 11 attacks, and the FBI's participation in various Department counterterrorism task forces.

In addition, the OIG currently is examining the FBI's observations of alleged mistreatment of detainees at military detention facilities, the FBI's compliance with the Attorney General Guidelines governing the use of confidential informants and other investigative techniques, and the FBI's handling of the Brandon Mayfield matter.

In this statement, I provide a summary of the findings of these completed reviews, as well as a description of ongoing OIG reviews in the FBI. In particular, I provide the findings of a follow-up audit, publicly released today, that examines the FBI's foreign language translation program and the backlog of unreviewed counterterrorism and counterintelligence foreign language audio material.

At the outset of my testimony, I want to offer my observations on the FBI and the key challenges it faces. These observations are based on numerous OIG reviews, as well as my more than 10 years in the OIG interacting with the FBI, the last 5 years as Inspector General.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00282 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.223

It is clear that the FBI is undergoing significant transformation on multiple fronts simultaneously, a difficult task in any large organization. The FBI's transformation will not happen immediately or easily. A variety of OIG reviews, many of which I summarize in this statement, have identified shortcomings in the FBI's efforts to remake itself and have highlighted areas in need of greater progress. However, despite the deficiencies we have found, I believe that Director Mueller is a strong leader who is moving the FBI in the right direction. Moreover, the FBI has been receptive to the recommendations in our reports and generally has agreed with the need to implement most of them.

I also want to note that while the OIG has described problems in a number of important FBI programs over the years, this should in no way diminish the contributions that dedicated FBI employees make on a daily basis. Many FBI employees throughout the country and the world perform their jobs diligently, often under very difficult circumstances, and their work is essential to the safety and security of the country.

However, there are several areas that I believe need significant improvement. The first is the urgent need to upgrade the FBI's information technology systems. In essence, the FBI is in the business of uncovering, analyzing, sharing, and acting on information. To do so effectively, it must have adequate information technology and case management systems. But the FBI's current information technology systems are far short of what is needed. As we have reported in several reviews, the FBI's efforts to create a modern case management system to catalogue, retrieve, and share case information throughout the agency have still not succeeded. Past OIG reports have described the problems the FBI's inadequate systems have created, such as our report describing the belated production of documents in the McVeigh case and the report on the FBI's handling of intelligence information related to the September 11 attacks. I believe that the upgrade of the FBI's information technology systems is one of the most critical challenges facing the FBI. Without adequate systems, the FBI will not be able to perform its job as effectively and fully as it should.

Second, the FBI faces challenges in the human capital area. I believe that some of the problems we found in our various reviews stem from high turnover in important positions throughout the FBI. We often see FBI employees in leadership positions for short periods of time. For example, turnover in key positions has hurt the FBI's ability to manage and oversee the Trilogy information technology modernization project. Between November 2001 and February 2005, 15 different key information technology managers have been involved with the Trilogy project, including 5 FBI Chief Information Officers and 10 individuals serving as project managers for various aspects of Trilogy. This lack of continuity contributed to the ineffective and untimely

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00283 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.224

implementation of the Trilogy project. Similarly, the FBI's counterterrorism division has had five leaders in the last four years. We also have seen rapid turnover in FBI field office managers. While some turnover is healthy in any organization, the rapid change in important positions throughout the FBI is unduly high, and I believe this turnover affects the FBI's ability to transform itself and fulfill its mission.

A third critical challenge facing the FBI is its need to share intelligence and law enforcement information efficiently, both within the FBI and with its law enforcement and intelligence partners. The FBI has made progress over the past several years in this area. For example, the OIG's review of Joint Terrorism Task Forces found that the FBI has made strides in sharing information with state and local partners, who are critical to the nation's counterterrorism efforts. But more must be done, particularly with regard to sharing intelligence information with other federal agencies. The FBI is only part of the nation's counterterrorism and counterintelligence efforts, and it must share its information effectively with other agencies.

Fourth, I believe the FBI must value and support to a greater degree FBI staff with technical skills. For example, until recently, the FBI did not adequately value the contributions of intelligence analysts. The FBI's general view was that special agents performed the key work of the agency, and intelligence analysts were used primarily to support ongoing cases. Special agents historically were promoted to technical leadership positions within the FBI, such as handling information technology upgrades or leading scientific efforts in the laboratory. While this culture is changing, more needs to be done to support the work of intelligence analysts, scientists, linguists, and other staff who are critical to meeting the FBI's changing mission and duties.

Fifth, I believe the FBI and Director Mueller should receive credit for opening the FBI to outside scrutiny much more than in the past. The FBI previously had an insular attitude, with an aversion to outside scrutiny or oversight. For example, until 2001, allegations of misconduct against FBI employees were not subject to outside review by the OIG, but were handled in-house by the FBI.

I believe the FBI's attitude is changing. As described below, the OIG now has jurisdiction to investigate misconduct in the FBI, and we have received good cooperation from the FBI in this new role. The FBI also has opened its programs and management to outside scrutiny from groups such the National Academy of Public Administration, the General Accountability Office, and other oversight entities. In addition, the FBI now is more willing to seek outside advice and support.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00284 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.225

Not everyone in the FBI has welcomed such change and outside scrutiny with open arms. But I believe that senior FBI leadership and most FBI employees recognize the need for such change and see the benefit of outside oversight. Director Mueller deserves credit for promoting this change in attitude throughout the FBI, even though the transformation is not yet complete.

Based on the many reviews of the FBI conducted by the OIG, I believe the FBI faces significant challenges and needs to make greater progress in many important areas. In this statement, I discuss several OIG reviews that provide a window on the challenges confronting the FBI, where it has made progress, and where additional improvement is needed.

My statement is organized in three main parts. In the first section, I provide background information on the OIG's oversight responsibilities in the FBI and how these responsibilities have changed. Second, I summarize the results of an important follow-up review that the OIG publicly issued today examining the FBI's progress in addressing findings in a July 2004 OIG audit on the FBI's foreign language translation program. Third, I briefly summarize the results from a series of recent OIG reviews of FBI programs and several ongoing reviews.

I. INSPECTOR GENERAL OVERSIGHT OF THE FBI

The OIG accomplishes its oversight responsibilities in the FBI through audits, inspections, investigations, and special reviews. The OIG's Investigations Division investigates allegations of criminal and administrative misconduct throughout the entire Department of Justice (DOJ or Department), including in the FBI. The OIG's Audit Division conducts audits of FBI programs and activities, including audits of the FBI's annual financial statements and computer security audits of FBI information technology systems. The OIG's Evaluation and Inspections Division conducts program reviews to assess the effectiveness of FBI operations. The OIG's Oversight and Review Division uses attorneys, investigators, and program analysts to conduct systemic reviews involving FBI programs or allegations of misconduct involving senior FBI officials.

Since its creation in 1989, the OIG has had the authority to conduct audits and inspections throughout all DOJ components. However, until July 2001, the OIG did not have jurisdiction to investigate allegations of misconduct in the FBI or the Drug Enforcement Administration (DEA). The FBI and DEA conducted their own investigations of employee misconduct. On July 11, 2001, the Attorney General expanded the OIG's authority to investigate allegations of misconduct in the FBI and the DEA. In

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00285 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.226

November 2002, Congress codified the OIG's authority to investigate allegations of misconduct involving FBI and DEA employees.[1]

Similar to other DOJ components, the OIG now reviews all allegations of misconduct against FBI employees and investigates the most serious ones, including allegations that if proved would result in prosecution and serious allegations against high-level FBI employees. We normally refer other allegations back to the FBI for it to handle, as we do with other DOJ components. While the FBI initially was not enthusiastic about the OIG's expanded jurisdiction to investigate misconduct allegations against its employees, I am pleased to report that it has cooperated well with OIG investigations, both at FBI headquarters and in the field.

In addition to investigating allegations of serious employee misconduct, the OIG plays an important role in ensuring that FBI whistleblowers who raise concerns about potential problems at the FBI are not retaliated against for raising these concerns. Although FBI employees are specifically excluded from the Whistleblower Protection Act (which covers most other federal employees), Congress provided a separate process to protect FBI employees from retaliation for making whistleblower disclosures. See 5 U.S.C. § 2303 and the implementing regulations in 28 C.F.R. Part 27. If FBI employees believe that the FBI has retaliated against them for making a protected disclosure, they may report the alleged reprisal to the OIG or DOJ OPR, which shares responsibility for investigating these reprisal allegations.

II. FBI FOREIGN LANGUAGE TRANSLATION PROGRAM

I now summarize the results of an important follow-up audit that the OIG completed and released today regarding the FBI's foreign language translation program. The FBI's ability to translate foreign language materials is critical to national security. These foreign language translations support the FBI's two highest investigative priorities – counterterrorism and counterintelligence – as well as its criminal and cyber-crimes programs.

In July 2004, the OIG completed a 157-page audit examining the FBI's foreign language translation program. That audit analyzed the backlog of unreviewed Foreign Intelligence Surveillance Act (FISA) material; the FBI's progress in hiring qualified linguists to translate critical foreign language materials; the FBI's prioritization of its translation workload; and the FBI's Quality Control Program for linguists.

[1] There is only one exception to the OIG's investigative jurisdiction throughout the Department. The OIG does not have authority to investigate allegations of misconduct involving DOJ attorneys acting in their capacity to litigate, investigate, or provide legal advice or investigators working under the direction of DOJ attorneys. That responsibility is given to the Department's Office of Professional Responsibility (DOJ OPR).

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00286 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.227

The July 2004 audit found that the FBI's collection of material requiring translation had outpaced its translation capabilities, and therefore the FBI could not translate all its foreign language counterterrorism and counterintelligence material. The audit also found that the FBI had difficulty in filling its need for additional linguists. In addition, the audit reported that the FBI's digital audio collection systems had limited storage capacity and that untranslated audio sessions were sometimes deleted from the system to make room for new incoming audio sessions. The audit found that the FBI was not in full compliance with the standards it had adopted for quality control reviews of the work of newly hired linguists, as well as annual reviews of permanent and contract linguists. The report made 18 recommendations to help the FBI improve its foreign language translation operations, and the FBI generally agreed to implement these changes.

To evaluate the FBI's progress in responding to the findings and recommendations in the July 2004 audit report, the OIG conducted a follow-up review in March and April of this year. In sum, our follow-up review concluded that the FBI has taken important steps to address the OIG's recommendations from the July 2004 audit and has made progress in improving the operations of the foreign language translation program. For example, the FBI now sets specific target staffing levels for linguists that account for attrition and, as of March 30, 2005, has achieved 56 percent of its hiring goals. In addition, although we found during our follow-up review that unreviewed translation materials still were being deleted, no unreviewed counterterrorism or Al Qaeda sessions had been deleted.

However, we found that key deficiencies remain in the FBI's foreign language translation program, including a continuing backlog of unreviewed material, some instances where high-priority material has not been reviewed within 24 hours in accordance with FBI policy, and continued challenges in meeting linguist hiring goals. In addition, implementation of the Quality Control Program for linguists has been slow. I will now discuss in more detail the main findings of this follow-up review.

A. Foreign Language Translation Workload and Unreviewed Material

Our follow-up review assessed the FBI's progress since our July 2004 report in addressing the volume of unreviewed counterterrorism and counterintelligence audio material ("backlog") that the FBI collects in its National Foreign Intelligence Program.

Our July 2004 report found the FBI had a significant backlog in translating counterterrorism and counterintelligence v audio material.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00287 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.228

Similarly, our follow-up review found that the FBI's collection of audio material continues to outpace its ability to review and translate all that material.

Table 1 provides an update on the FBI's backlog. It provides the amount of audio collected and unreviewed through the end of the first quarter of FY 2004 (as of December 31, 2003), and then through the end of the second quarter of FY 2005 (as of March 31, 2005).

Table 1: TOTAL AUDIO COLLECTED AND UNREVIEWED

Program	Accrued Unreviewed Audio FY 2002 through 1st Quarter FY 2004 (Hours)	Audio Collected FY 2002 through 1st Quarter FY 2004 (Hours)	Percent Unreviewed of Collected	Accrued Unreviewed Audio FY 2002 through 2nd Quarter FY 2005 (Hours)	Audio Collected FY 2002 through 2nd Quarter FY 2005 (Hours)	Percent Unreviewed of Total Collected
Counterterrorism	24,786	354,014	7%	38,514	573,920	7%
Counterintelligence	453,787	1,322,773	34%	669,228	2,015,998	33%
Total	478,573	1,676,787	29%	707,742	2,589,918	27%

Source: OIG calculations based on FBI Language Services Section data.

As Table 1 demonstrates, the total collections of counterterrorism and counterintelligence audio material increased from approximately 1.6 million hours as of December 31, 2003, to approximately 2.5 million hours as of March 31, 2005. During the same time period, the total amount of unreviewed audio increased from 478,573 hours to 707,742 hours. As a percentage of total collections, the percentage of unreviewed audio material remained relatively constant, only slightly decreasing from 29 percent to 27 percent.

Counterterrorism Material. As also shown in Table 1, the FBI reported in its monthly counterterrorism FISA surveys that the accrued unreviewed counterterrorism audio was 24,786 hours as of December 31, 2003, and increased to 38,514 hours as of March 31, 2005.

However, in its monthly surveys the FBI refines the amount of counterterrorism audio that the FBI's data collection system reports as unreviewed. The FBI tries to eliminate double counting of unreviewed material by more than one field office, unreviewed material in cases that are no longer active, and collections of materials from the wrong sources due to technical problems. To attempt to determine the amounts of unreviewed material that should be eliminated on the monthly surveys, FBI field offices submit what they believe is their total accrued backlog after eliminating these items. The FBI then accumulates the field offices' submissions to reach a more refined estimate of the total amount of unreviewed counterterrorism audio material.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00288 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.229

According to this method, our July 2004 audit reported that the FBI's estimated counterterrorism audio backlog was 4,086 hours as of April 2004. In this follow-up review, according to this same method, we found that as of March 2005 the counterterrorism audio backlog had increased to 8,354 hours.

According to this method, the counterterrorism backlog represented 1 percent of all counterterrorism audio collected as of April 2004. As of March 2005, the counterterrorism backlog had increased to 1.5 percent of all counterterrorism audio collected.

In our follow-up review, we also attempted to determine the priority of the counterterrorism audio material that was not reviewed. The FBI designates one of five levels of priority to its counterterrorism cases. We found that none of the counterterrorism audio backlog as of March 2005 was in the highest level priority cases. However, almost all of the 8,354 hours of counterterrorism backlog reported by the FBI was in cases designated in the second and third highest priority levels: 72 percent of this backlog was in the FBI's second highest priority counterterrorism cases, and 27 percent was in the third highest priority.

Counterintelligence Material. With respect to counterintelligence material, as Table 1 shows, total collections increased from approximately 1.3 million hours as of December 31, 2003, to approximately 2 million hours as of March 31, 2005. The amount of unreviewed counterintelligence material increased from 453,787 hours to 669,228 hours during this same period. The percentage of unreviewed counterintelligence material remained relatively constant, decreasing only slightly from 34 percent to 33 percent.

In response to these statistics on unreviewed material, the FBI stated that it collects significant amounts of FISA audio material that it does not intend to translate, either immediately or possibly ever. For example, it stated that the FBI's digital collection systems cannot reliably filter out "white-noise" (acoustical or electrical noise) and unintelligible audio, which is collected but does not need to be reviewed. In addition, the FBI stated that in many counterintelligence cases it collects audio material that it stores and only translates if additional information points to those materials as containing significant information that should be reviewed. It also stated that it believes that most of the unreviewed counterintelligence backlog fell into these categories, but it was unable to quantify the amounts of unreviewed material that fell into these different categories.

In addition, during our follow-up review we performed testing to determine if the FBI was reviewing material designated as "high priority" within 24 hours. Our testing of eight FBI field offices for three separate days in

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00289 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.230

April 2005 found that three offices had not reviewed all high-priority material within 24 hours on all three dates.

As we described in our July 2004 report, because the FBI field offices' digital collection systems have limited storage capacity, audio sessions resident on a system were sometimes deleted through an automatic file deletion procedure to make room for incoming audio sessions. Although these sessions are archived, it is difficult for the FBI to determine, once the sessions have been deleted and archived, whether they have been reviewed. We found that sessions are automatically deleted in a set order, and unreviewed sessions are sometimes included in the material deleted, especially in offices with a high volume of audio to review.

In our July 2004 audit, we reported that the results of our tests showed that three of eight offices tested had Al Qaeda sessions that potentially were deleted by the system before linguists had reviewed them. We recommended that the FBI establish controls to prevent critical audio material from being deleted.

During our follow-up review this year, we tested data for eight offices to determine if unreviewed translation material was still being deleted. The results of our testing showed unreviewed counterintelligence material had been deleted and archived at six of the eight offices. However, no unreviewed counterterrorism or Al Qaeda sessions had been deleted at the eight offices.

B. Hiring of Linguists and Quality Control Program

As reported in our July 2004 audit report, the number of FBI and contract linguists had increased from 883 in FY 2001 to 1,214 as of April 2004. Since then, the number of FBI and contract linguists has increased to 1,338 as of March 30, 2005.

We found that the FBI has made progress in improving its hiring process since our July 2004 review, although it still continues to face challenges hiring linguists. The FBI met 62 percent of its hiring goals for FY 2004, and as of March 30, 2005, met 56 percent of its hiring goals in FY 2005.

A continuing issue for the FBI is the time it takes to hire contract linguists. Since our July 2004 audit, according to the FBI, the average time it takes the FBI to hire a contract linguist has increased by at least 1 month, from 13 months to 14 months. However, according to our review of the FBI's data, it now takes the FBI 16 months on average to hire a contract linguist.

With regard to quality control issues, in response to our July 2004 report the FBI modified its Translation Quality Control Policy and Guidelines, effective

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00290 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.231

December 30, 2004. The modified policy and guidelines now require, for example, the use of certified reviewers, anonymous reviews, and the review of randomly selected materials marked as "Not Pertinent" by a linguist in addition to review of summary and verbatim translations.

However, during the fieldwork for our follow-up review in March 2005, the FBI still had no nationwide system in place to ensure that FBI field offices were performing quality control reviews or were monitoring results of the reviews. In July 2005, just before our follow-up report was issued, the FBI stated that it had implemented a tracking system for monitoring the reviews and the results of those reviews.

In sum, since issuance of the July 2004 report the FBI has taken significant steps to address many of our recommendations and has made progress in improving the operations of its foreign language translation program. But key deficiencies remain, including the continuing amount of unreviewed material, instances where "high priority" material has not been reviewed within 24 hours, and continued challenges in meeting linguist hiring goals. With regard to unreviewed material, our follow-up review found that the FBI's collection of audio material continues to outpace its ability to review and translate that material, and the amount of unreviewed FBI counterterrorism and counterintelligence audio material has increased since our July 2004 report. According to the FBI's calculations, the backlog of unreviewed counterterrorism material represents 1.5 percent of total counterterrorism audio collections, although the amount of unreviewed counterintelligence material is larger. While the FBI stated that most of the unreviewed materials may not need to be translated, it has no assurance that all of this counterterrorism and counterintelligence material need not be reviewed or translated.

III. ADDITIONAL OIG REVIEWS OF FBI PROGRAMS

A. Recently Completed OIG Reviews

Management of the Trilogy Information Technology Modernization Project: The Trilogy project was intended to be the centerpiece of the FBI's efforts to upgrade its information technology infrastructure and replace its antiquated paper-based case management system with a new electronic case management system called the Virtual Case File (VCF). Trilogy consisted of three main components: 1) the Information Presentation Component intended to upgrade the FBI's hardware and software; 2) the Transportation Network Component intended to upgrade the FBI's communication networks; and 3) the User Applications Component intended to replace the FBI's most important investigative applications, including the Automated Case Support (ACS) system, the FBI's current case management system. The first two components

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00291 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.232

of Trilogy provide the infrastructure needed to run the FBI's various user applications, including the planned VCF.

It is important to note that Trilogy was not intended to replace all of the FBI's investigative applications or all of the FBI's other non-investigative applications. Rather, Trilogy was intended to lay the foundation so that future enhancements would allow the FBI to achieve a state-of-the-art information technology system that integrates all of the agency's investigative and non-investigative applications.

A February 2005 OIG audit reported that the FBI had successfully completed the Trilogy infrastructure upgrades, albeit with significant delays and cost increases. The infrastructure upgrades included deploying new hardware and software, and new communications networks. However, this deployment was completed 22 months later than expected, despite an additional $78 million provided by Congress after the September 11 terrorist attacks to accelerate deployment of Trilogy's infrastructure components. In addition, the total costs for the infrastructure components of Trilogy increased from $238.6 million to $337 million over the course of the project.

With regard to the VCF, the third phase of Trilogy, the FBI was unable to create and deploy the VCF after more than 3 years and $170 million budgeted for the project. The OIG audit report concluded that the VCF either would require substantial additional work or would need to be scrapped and replaced by a new system. Moreover, at the time of the audit, the FBI had not provided a realistic timetable or cost estimate for implementing a workable VCF or a successor system.

The OIG audit identified a variety of causes for the delays and cost increases in the Trilogy project, including poorly defined and slowly evolving design requirements for Trilogy, weak information technology investment management practices at the FBI, weaknesses in the way contractors were retained and overseen, the lack of management continuity at the FBI on the Trilogy project, unrealistic scheduling of tasks on Trilogy, and inadequate resolution of issues that warned of problems in Trilogy's development.

The OIG report concluded that responsibility for ensuring the success of the Trilogy project was shared by several parties: the FBI; the Department; FEDSIM (the component of the General Services Administration that awarded Trilogy contracts on behalf of the FBI); and the two contractors – Computer Sciences Corporation for the two infrastructure components, and Science Applications International Corporation for the user applications component that included the VCF. These entities, to varying degrees, did not effectively contract for, manage, monitor, or implement the Trilogy project.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00292 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.233

However, the OIG report faulted the FBI for moving forward with contracting for this complex project without providing or insisting upon defined requirements, specific milestones, critical decision review points, and penalties for poor contractor performance. Because of the FBI's inability to develop and deploy the VCF, the audit concluded that the FBI continued to lack critical tools necessary to maximize the performance of both its criminal investigative and national security missions.

In March 2005, the FBI announced that is was terminating the VCF and replacing it with a new information technology effort called Sentinel. The FBI believes that Sentinel, through a phased approach, will result in a system that will provide an automated workflow process, search capabilities, and an effective records and case management system. At the request of the FBI Director and Congress, the OIG is continuing its audits of the FBI's information technology upgrade efforts, including an ongoing review of Sentinel. A description of that ongoing OIG audit is provided in the next section of this statement.

The Handling of Intelligence Information Prior to the September 11 Attacks: On June 7, 2005, the unclassified, redacted version of the OIG's report that examined the FBI's handling of intelligence information related to the September 11 attacks was released publicly. The OIG report examined what intelligence information the FBI had prior to the September 11 attacks that potentially was related to those attacks. Among other issues, the OIG examined the FBI's handling of the Zacarias Moussaoui case; the FBI's handling of an Electronic Communication written by an FBI agent in Phoenix, Arizona (the Phoenix EC) that raised concerns about efforts by Usama Bin Laden to send students to attend United States civil aviation schools to conduct terrorist activities; and intelligence information available to the FBI regarding two of the September 11 hijackers – Nawaf al Hazmi and Khalid al Mihdhar.

In July 2004, the OIG completed and issued its full report, classified at the Top Secret/SCI level, to the Department, the FBI, Congress, the Central Intelligence Agency (CIA), the National Security Agency, and the National Commission on Terrorist Attacks Upon the United States (9/11 Commission). In its final report, the 9/11 Commission referenced the findings from the OIG's report.

After the OIG issued the classified version of our report, several members of this Committee asked the OIG to create and release publicly an unclassified version because of the significant public interest in these matters. The OIG therefore created a 371-page unclassified version of the report. However, because Moussaoui is being prosecuted before the United States District Court for the Eastern District of Virginia, the rules of that Court prevented the OIG

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00293 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.234

from releasing the unclassified report without the permission of the District Court. The District Court denied the OIG's motion to release publicly the full unclassified version of the report in late April 2005. The OIG redacted from the unclassified report the information requested by Moussaoui's defense counsel that related to Moussaoui and other matters. The Court subsequently granted the OIG's motion to release the redacted report.

The OIG's redacted, unclassified report details the FBI's handling of the Phoenix EC and the systemic problems that the handling of this EC revealed about the FBI's operations. The redacted report also discusses the FBI's handling of the Hazmi/Mihdhar case. The FBI also had at least five opportunities to uncover information regarding the presence of Hazmi and Mihdhar in the United States that could have led the FBI to seek to find them before the September 11 attacks. The report describes the systemic impediments that hindered the sharing of information between the FBI and the CIA, and the report assesses the individual performance of FBI employees. The report also contains the OIG's recommendations and conclusions relating to the FBI's analytical program, the FISA process, the FBI's interactions with other members of the Intelligence Community, and other matters involved in this review.

In sum, the OIG review found significant deficiencies in the FBI's handling of intelligence information related to the September 11 attacks. Our review concluded that the FBI failed to fully evaluate, investigate, exploit, and disseminate information related to the Phoenix EC and the Hazmi and Mihdhar matter. The causes for these failures were widespread and varied, ranging from poor individual performance to more substantial systemic deficiencies that undermined the FBI's efforts to detect and prevent terrorism.

In its response to the OIG's report, the FBI described changes it has made related to these issues since the September 11 attacks. In addition, the FBI has created a panel to assess whether any action should be taken with regard to the performance of FBI employees described in the OIG report.

Terrorist Screening Center: The OIG reviewed the FBI's management of the Terrorist Screening Center (TSC), a multi-agency effort to consolidate the federal government's terrorist watch lists and provide 24-hour, 7-day-a-week responses for screening individuals against the consolidated watch list. Prior to establishment of the TSC, the federal government relied on many separate watch lists maintained by a variety of agencies to search for terrorist-related information about individuals who, among other things, apply for a visa, attempt to enter the United States through a port of entry, travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation. The FBI is responsible for managing the TSC and the efforts to develop an accurate consolidated watch list.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00294 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.235

The OIG review found that the TSC has made significant strides in creating a new organization and a consolidated watch list, which was a significant accomplishment. However, the OIG review also concluded that the TSC needs to address weaknesses in its consolidated terrorist watch list database, computer systems, as well as staffing, training, and oversight of the call center.

The OIG concluded that the TSC has not ensured that the information in that database is complete and accurate. For example, the OIG found instances where the consolidated database did not contain names that should have been included on the watch list and inaccurate or inconsistent information related to persons included in the database.

The OIG also found problems with the TSC's management of its information technology, a critical part of the terrorist screening process. From its inception, the TSC's Information Technology Branch – staffed with numerous contractors – did not provide effective leadership over the agency's information technology functions. In addition, the TSC has experienced significant difficulty in hiring qualified staff with adequate security clearances to perform information technology functions.

The OIG report offered 40 recommendations to the TSC to address areas such as database improvements, data accuracy and completeness, call center management, and staffing. The TSC generally agreed with the recommendations and in some cases provided evidence that it has taken action to correct the weaknesses that the audit identified.

The OIG currently is conducting a follow-up review that examines the TSC's plans to support the Secure Flight Program, which is currently under development in the Transportation Security Agency (TSA). The Secure Flight Program will compare domestic airline passenger information to the consolidated terrorist watch list. The OIG is examining the TSC's plans to support the Secure Flight program in light of a pending congressional request from the TSC for an additional $75 million budget increase in fiscal year 2006. The OIG intends to complete a report with the results of our review by August 1, 2005.

FBI Efforts to Hire, Train, and Retain Intelligence Analysts: In May 2005, the OIG issued a 173-page audit that examined FBI efforts to hire, train, and retain intelligence analysts. Since the September 11 terrorist attacks, the FBI has attempted to hire, train, and use more fully qualified intelligence analysts. In the three years since the attacks, the number of FBI analysts has grown from 1,023 analysts in October 2001 to 1,403 analysts in October 2004 – a net increase of 380 intelligence analysts, or 37 percent.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00295 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.236

Yet, the OIG report found that while the FBI has made progress in hiring and training intelligence analysts, several areas are in need of improvement. For example, the FBI fell short of its fiscal year (FY) 2004 hiring goal by 478 analysts and ended the fiscal year with a vacancy rate of 32 percent. At the end of FY 2004, the FBI had hired less than 40 percent of its goal of 787 analysts.

The audit found that the analysts that the FBI hired generally were well qualified. But the FBI has made slow progress toward developing a quality training curriculum for new analysts. The initial basic training course offered to analysts from 2002 to 2004 was not well attended and received negative evaluations. As a result, the FBI initiated a revised 7-week training course in September 2004.

FBI analysts who responded to an OIG survey indicated that they generally were satisfied with their work assignments, believed they made a significant contribution to the FBI's mission, and were intellectually challenged. However, newer and more highly qualified analysts were more likely to respond negatively to OIG survey questions on these issues. For example, 27 percent of the analysts hired within the last five years reported dissatisfaction with their work assignments compared to 13 percent of the analysts hired more than five years ago.

Further, the intelligence analysts reported on the survey that work requiring analytical skills accounted for about 50 percent of their time. Many analysts reported performing administrative or other non-analytical tasks, such as escort and phone duty. In addition, some analysts said that not all FBI Special Agents, who often supervise analysts, understand the capabilities and functions of intelligence analysts.

The OIG report made 15 recommendations to help the FBI improve its efforts to hire, train, and retain intelligence analysts, including recommendations that the FBI establish hiring goals for intelligence analysts based on the forecasted need for intelligence analysts and projected attrition; implement a better methodology for determining the number of intelligence analysts required and for allocating the positions among FBI offices; and assess the work done by intelligence analysts to determine what is analytical in nature and what general administrative support of investigations can more effectively be performed by other support or administrative personnel. The FBI agreed with the OIG recommendations.

Department of Justice Counterterrorism Task Forces: In a June 2005 report, the OIG examined the operation of DOJ Counterterrorism task forces and whether gaps, duplication, or overlap existed in task forces' work. Three of

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00296 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.237

the five groups we examined – the Joint Terrorism Task Forces (JTTFs), the National Joint Terrorism Task Force, and the Foreign Terrorist Tracking Task Force – are led by the FBI.

The OIG review concluded that the terrorism task forces generally functioned well, without significant duplication of effort, and that they contributed significantly to the Department's goal of preventing terrorism. However, the OIG review identified a series of management and resource problems affecting the operation of the task forces. These included the need for more stable leadership among the task forces, better training for participants, and additional resources. For example, many JTTF members stated that frequent turnover in leadership of the JTTFs affected the structure and stability of the JTTFs and their terrorism investigations.

In addition, the review found that the urban-based JTTFs do not consistently coordinate their activities to share information with the law enforcement agencies and first responders in rural and remote areas within their jurisdictions. We also found that the FBI has not signed Memorandums of Understanding defining the roles, responsibilities, and information-sharing protocols with all of the agencies participating on the task forces. The OIG report provided 28 recommendations to help the FBI and the Department improve the operations of its various counterterrorism task forces. The FBI generally agreed with the recommendations and agreed to take corrective action.

Follow-up Review of the Status of IDENT/IAFIS Integration: In December 2004, the OIG completed a report that examined efforts to integrate the federal government's law enforcement and immigration agencies' automated fingerprint identification databases. Fully integrating the automated fingerprint system operated by the FBI (IAFIS) and the system operated by the Department of Homeland Security (IDENT) would allow law enforcement and immigration officers to more easily identify known criminals and known or suspected terrorists trying to enter the United States, as well as identify those already in the United States. The December 2004 report was the fifth OIG report in 4 years that monitors the progress of efforts to integrate IAFIS and IDENT.

The December 2004 OIG report found that the congressional directive to fully integrate the federal government's various fingerprint identification systems has not been accomplished because of high-level policy disagreements among the Departments of Justice, Homeland Security, and State regarding such integration. The key policy disagreement was a dispute over how many fingerprints should be taken from foreign visitors to the United States for enrollment into the Department of Homeland Security's (DHS) US-VISIT system.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00297 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.238

Our December 2004 report made six recommendations to the Department, four of which were directed to the FBI. The report again recommended that the Departments of Justice and Homeland Security enter into a Memorandum of Understanding to guide the integration of IAFIS and IDENT.

The FBI has been addressing our recommendations, including the recommendation to increase its transmission of fingerprints of known or suspected terrorists to the DHS from monthly to weekly and identifying the costs and capacity needed to upgrade IAFIS. In April 2005, we learned that the federal government's Homeland Security Committee had adopted a uniform federal biometric standard of ten fingerprints for enrollment. Accordingly, in July 2005, in connection with a restructuring of the DHS, the DHS announced that it would require US-VISIT – which currently takes two fingerprints for enrollment and identify verification – to begin taking ten fingerprints from visitors upon initial entry into the United States, with continued use of two fingerprint verification for subsequent entry. We believe these steps address our recommendation and should facilitate the development of interoperable automated fingerprint identification systems.

DNA Reviews: In 2004, the OIG completed two reviews examining various aspects of DNA issues. In the first review, completed in May 2004, the OIG examined vulnerabilities in the protocols and practices in the FBI's DNA Laboratory. This review was initiated after it was discovered that an examiner in a DNA Analysis Unit failed to perform negative contamination tests, and the Laboratory's protocols had not detected these omissions. The OIG's review found that certain of the FBI Laboratory's DNA protocols were vulnerable to undetected, inadvertent, or willful non-compliance by DNA staff, and the OIG report made 35 recommendations to address these vulnerabilities. The FBI agreed to amend its protocols to address these recommendations and to improve its DNA training program.

In a second review, the OIG audited laboratories that participate in the FBI's Combined DNA Index System (CODIS), a national database maintained by the FBI that allows law enforcement agencies to search and exchange DNA information. The OIG's CODIS audits identified concerns with some participants' compliance with quality assurance standards and with their uploading of unallowable and inaccurate DNA profiles to the national level of CODIS.

Effects of the FBI's Reprioritization: In a September 2004 report, the OIG reviewed the changes in the FBI's allocation of its personnel resources since the September 11 terrorist attacks. The report provided detailed statistical information regarding changes in the FBI's allocation of resources since 2000.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00298 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.239

The OIG found that the FBI has reallocated resources in accord with its shift in priorities from traditional criminal investigative work to counterterrorism and counterintelligence matters. In addition, the OIG identified FBI field offices most affected by changes in FBI priorities within various investigative areas, such as shifting agent resources from organized crime or health care fraud cases to terrorism investigations. The OIG report recommended that the FBI regularly conduct similar detailed analyses of its agent usage and case openings to provide a data-based view of FBI operations and to assist managers in evaluating the FBI's progress in meeting its goals.

The September 2004 OIG review is the second in a series of three reviews that examines the FBI's reprioritization efforts since the September 11 terrorist attacks. In a report released in September 2003, the OIG examined the FBI's use of personnel resources in its investigative programs over an almost 7-year period, 6 years before the September 11 terrorist attacks and 9 months after the attacks. The report compared the actual usage of resources to the FBI's planned allocation of resources during this same October 1995 to June 2002 time period. It also examined the types and numbers of cases the FBI investigated during these 7 years.

The OIG currently is working on a third review examining how the FBI's reprioritization efforts and the shift of resources from more traditional criminal investigative areas such as drugs and white collar crime to terrorism has affected other federal, state, and local law enforcement organizations. As part of this review, we distributed a web-based survey to approximately 3,500 state and local agencies, and we conducted interviews with federal, state, and local officials.

Efforts to Improve the Sharing of Intelligence and Other Information: In a report issued in December 2003, the OIG reviewed the FBI's efforts to improve the sharing of intelligence and other information. The review found that among the FBI's main obstacles to effective information sharing were the need to improve its information technology systems, enhance its ability to analyze intelligence, overcome security clearance and other security issues concerning the sharing of information with state and local law enforcement agencies, and develop policies and procedures for managing information sharing within the FBI.

Since the report's issuance, the FBI has taken various actions in response to the report's recommendations. The FBI has drafted an Intelligence Dissemination Policy Manual to provide consistent procedures for information sharing, including what types of information should be shared with what parties under what circumstances; completed a blueprint and process map for intelligence and information sharing; and revised its policy for Urgent Reports

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00299 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.240

that are submitted by field offices to the FBI Director regarding critical matters requiring immediate attention.

However, we remain concerned about the overall effectiveness of FBI information sharing. The FBI's ability to rapidly and fully share investigative information is limited because of its inability to implement the VCF. We also are reviewing whether the procedures the FBI implemented in response to our December 2003 audit have been sufficiently comprehensive and effective in ensuring that all relevant FBI employees receive and adequately disseminate intelligence reports.

B. Ongoing OIG Reviews in the FBI

The OIG currently is conducting reviews of a variety of FBI programs. The following are examples of ongoing OIG reviews in the FBI:

FBI Observations of and Reports Regarding Detainee Treatment at Military Facilities: The OIG currently is examining FBI employees' observations and actions regarding alleged abuse of detainees at Guantanamo Bay, Iraq, Afghanistan, and other venues controlled by the U.S. military. The OIG is investigating whether FBI employees participated in any incident of detainee abuse in military facilities at these locations, whether FBI employees witnessed incidents of abuse, how FBI employees reported observations of alleged abuse, and how those reports were handled by the FBI.

As part of this ongoing review, the OIG has interviewed detainees, FBI employees, and military personnel at Guantanamo. In addition, the OIG has administered a detailed questionnaire to approximately 1,000 FBI employees who served assignments at these locations. The questionnaire requested information on what the FBI employees observed, whether they reported observations of concern, and how those reports were handled. To date, the OIG has received over 900 responses to its questionnaire. The investigative team is also conducting appropriate follow-up interviews.

It is important to note that the actions of military personnel are not within the jurisdiction of the DOJ OIG and therefore are not the subject of the OIG's review. Rather, those actions are the subject of reviews by Department of Defense officials. However, the OIG is coordinating its work with a military review conducted by the U.S. Southern Command, which has been reviewing instances of alleged mistreatment of detainees at Guantanamo Bay that are cited in FBI documents.

Oversight of the FBI's Sentinel Case Management Project: In March 2005, the FBI announced plans to develop the Sentinel Case Management system to replace the Virtual Case File effort. The FBI stated that it hopes to

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00300 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.241

use modular off-the-shelf components for Sentinel and expects to implement the new case management system in 39 to 48 months. The FBI stated that it plans to issue a "Request for Proposals" to develop the system by September 2005, award the contract in late 2005, and begin development work in early 2006.

At the request of the FBI Director and Congress, the OIG intends to monitor and review the FBI's continuing efforts to upgrade its case management system and the implementation of its Sentinel project. We have begun a review of the Sentinel project and are initially focusing on the FBI's planning for the project, including the FBI's approach to developing the system, management controls over the project, information technology management processes, project baselines, contracting processes, and funding sources. Rather than issue a single audit report, we anticipate completing a series of follow-up audits about discrete aspects of the Sentinel project, such as the FBI's monitoring of the contractor's performance against established baselines and the overall progress of the project.

FBI's Handling of the Brandon Mayfield Matter: The OIG is investigating the FBI's conduct in connection with the erroneous identification of a fingerprint found on evidence from the March 2004 Madrid train bombing. The FBI's fingerprint examiners erroneously concluded that the fingerprint belonged to Brandon Mayfield, an attorney in Portland, Oregon. As a result of the misidentification, the FBI initiated an investigation of Mayfield that resulted in his arrest as a "material witness" and his detention for approximately two weeks. Mayfield was released when Spanish National Police matched the fingerprints on the evidence to an Algerian national. The OIG is examining the cause of the erroneous fingerprint identification and the FBI's handling of the matter, including the investigation of Mayfield. The Department of Justice Office of Professional Responsibility is reviewing the conduct of the prosecutors in the case.

In our review, the OIG has consulted with national fingerprint experts to assist in the evaluation of the causes for the fingerprint misidentification. The OIG report also will examine the corrective actions taken by the FBI Laboratory since the misidentification came to light. In addition, the OIG report will address issues arising from the FBI's investigation and arrest of Brandon Mayfield, including any use of or implication of the Patriot Act in this case, the FBI's participation in the preparation of the material witness and criminal search warrants, and Mayfield's conditions of confinement while he was held as a material witness. The OIG is nearing the completion of its review, and is currently drafting its report of investigation.

The FBI's Compliance with the Attorney General's Investigative Guidelines: The OIG is completing a review of the FBI's compliance with

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00301 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.242

Attorney General Investigative Guidelines governing the use of confidential informants; undercover operations; investigations of general crimes, racketeering enterprises, and terrorism enterprises; and warrantless monitoring of verbal communications. On May 30, 2002, the Attorney General approved revisions to each of the Guidelines. To assess the FBI's compliance with the revised Guidelines and to evaluate the procedures that the FBI employed to ensure that the revised Guidelines were properly implemented, the OIG conducted surveys of FBI field personnel and the Criminal Division Chiefs of the 93 U.S. Attorney Offices and visited 12 FBI field offices. We also conducted interviews of FBI Headquarters and DOJ personnel. The OIG's final report will make recommendations to promote compliance with the Attorney General Guidelines.

Follow-Up Review Regarding OIG Report on Espionage of Robert Hanssen: The OIG recently initiated a review of the FBI's progress in implementing the recommendations contained in the OIG's August 2003 report entitled, "Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen."

IV. CONCLUSION

In sum, I believe the FBI has made progress in addressing its changed priorities since the September 11 terrorist attacks. But significant challenges and deficiencies remain, as various OIG reports have found. The FBI needs more improvement in critical areas such as upgrading its information technology systems; hiring, training, and using intelligence analysts; timely and accurately reviewing and translating foreign language material; sharing information effectively within and outside the FBI; and ensuring continuity of personnel in key positions. While I believe that Director Mueller is leading the FBI in the right direction, the FBI needs to make significant improvements as it continues this transformation. To assist in this effort, the OIG will continue to monitor the FBI's progress and conduct reviews in important FBI programs.

This concludes my prepared statement, and I would be pleased to answer any questions.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00302 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.243

UNITED STATES SENATOR • IOWA
CHUCK GRASSLEY

http://grassley.senate.gov
grassley_press@grassley.senate.gov

Contact: Jill Kozeny, 202/224-1308
Beth Pellett, 202/224-6197
Dustin Vande Hoef, 202/224-0484

Prepared Opening Statement of Senator Chuck Grassley of Iowa
Senate Committee on the Judiciary
FBI Oversight Hearing
July 27, 2005

Thank you, Mr. Chairman, for holding this FBI oversight hearing today. There are many challenges facing the FBI and many questions about its role in the Global War on Terrorism. We are going to explore several problem areas today, including the failed attempt to modernize the FBI's computer system and the difficulties in hiring and screening essential foreign language translators. I want to thank Director Mueller, Inspector General Fine, and our other witnesses for being here today, and I look forward to hearing their testimony. However, Mr. Chairman, I hope this hearing is the first of a series, and I hope that future hearings will examine some of the individual issues raised today in greater detail. The devil is often in the details, which is why effective oversight of the FBI is so important for Congress and the public to understand what is really going on.

One of my biggest concerns is missed opportunities. Looking back on all the reports and reviews conducted after 9/11, it is those missed opportunities that are the most frustrating even recognizing the benefit of hindsight. What if the FBI had been searching earlier for the two hijackers that were living with an FBI informant in San Diego? What if they had devoted more resources to finding those two hijackers once they began looking for them? What if Zacharias Moussaoui's computer had been searched earlier? What if someone had done something in response to the Phoenix memo about foreign students at American flight schools? What if it had been more difficult for young men from countries that promote extremist ideologies to get a visa, overstay their welcome in the U.S., and obtain drivers licenses and other identification?

We need to do more than just look back and wonder, "what if?" We need to learn lessons from our mistakes and change our behavior so that we don't miss the opportunities to stop the next terrorist attack. Unfortunately, I continue to see the sort of problems that contribute to more missed opportunities.

Nearly four years after 9/11, the FBI still needs to shift its culture away from secrecy and turf wars to openness and real partnerships with other government agencies.

Earlier this year, I was contacted by the head of the Immigration and Customs Enforcement (ICE) office in Houston, Joe Webber, who reported that the FBI had delayed an ICE wiretap request on a suspected terrorist fundraiser. Mr. Webber alleged that FBI resistance to the wiretap request was motivated by a desire to protect FBI's turf as the "lead agency" on terrorist financing investigations. At a minimum, it is clear that a lack of coordination at the FBI caused

the government to miss an opportunity to intercept over 700 communications from a criminal suspect, including some with a designated terrorist.

I am continuing to try to learn more about this case, but have been disappointed by the lack of cooperation from the FBI. Field and headquarters personnel have given contradictory accounts of why the wiretap request was delayed, but unfortunately, the FBI has shown little interest in resolving those conflicting statements and getting to the bottom of what happened. I have asked the Inspector General to look into this matter as well, and I anxiously await his report. If anyone put protecting FBI turf ahead protecting America from terrorists, then they need to be held accountable.

The GAO recently reported that the FBI was not providing the State Department's passport office access to the Terrorist Screening Center (TSC) watch list or comprehensive information about wanted felons. That means that suspected terrorists and violent fugitives could apply for and obtain a U.S. passport without any red flags in the system. Even a member of the FBI's Ten Most Wanted could have gotten a passport. Only after GAO and Congress started asking questions did the FBI and the State Department develop an agreement to begin systematically sharing this vital information.

Nearly four years after 9/11, the FBI has failed to implement a modern computer system for case management. Such a system is essential for the various field offices and units within FBI headquarters to store and maintain information in a way that can be seamlessly accessed by others with counterterrorism responsibilities both inside and outside the FBI. Yet, the FBI wasted precious time and more than $180 million dollars on its Virtual Case File system before scrapping it and starting over on a new planned system called "Sentinel." We have not yet been told what the new system will cost, but we know it will be years before it is complete. It is also unclear to what degree Sentinel may duplicate functionality already being developed in the Consolidated Enforcement Environment (CEE), which will be used by the Departments of Homeland Security and Justice. We also don't have a clear understanding of what steps are being taken to ensure that the two systems will be compatible.

Nearly four years after 9/11, the FBI has failed to properly screen, hire, and manage an adequate number of translators of critical foreign languages. According to the Inspector General in a report issued last summer, electronic intercepts waiting in a backlog were being automatically deleted from the FBI's system before any translator had a chance to review them. Translators have been caught reviewing intercepts involving people they personally knew without disclosing that relationship to the FBI. Others have claimed that background checks on translators have been given short shrift because of the extreme need to hire as many as possible as quickly as possible.

We don't know what was on those recordings that were deleted before being translated. We don't know what that subject in Houston was discussing with a designated terrorist. And, we don't know whether anyone on the TSC terrorist watch list got a U.S. passport because FBI and State weren't sharing information. But, these are opportunities we cannot afford to miss. Unless the FBI culture is fixed, there will be more missed opportunities like these - any one of which might be the key to stopping the next major attack and saving American lives.

-30-

46051.245

Prepared Statement of
Former Vice Chair Lee H. Hamilton,
National Commission on Terrorist Attacks Upon the United States,
before the Senate Committee on the Judiciary
July 27, 2005

FBI Reform

Chairman Specter, Ranking member Leahy, distinguished members of the Senate Committee on the Judiciary: I am honored to appear before you today regarding the progress of reform at the FBI.

At the outset, I want to commend you for holding this hearing. Reform at the FBI benefits from your attention. Director Mueller needs your oversight. The spotlight you shine, and the guidance you provide, will help reform move forward.

I. Recommendations by the 9/11 Commission for Reform at the FBI

First, I would like to review briefly the recommendations of the 9/11 Commission with respect to the FBI, and the extent to which they have been implemented.

The Commission found significant shortfalls in the Bureau's capabilities. Chief among them was inadequate information sharing: the FBI's culture of law enforcement impeded its ability to gather and disseminate intelligence on terrorists before 9/11.

- The FBI was not able to link the knowledge of its agents in the field to national priorities.
- Information sharing was severely hindered by a computer system installed in 1995 that was based on 1980s technology.
- Two-thirds of the FBI's analysts were unqualified for their tasks; the Bureau never assessed the terrorist threat at home before 9/11.
- Key memos, such as the Phoenix memo expressing a concern about the "possibility of a coordinated effort by Usama Bin Laden" to send students to the United States to attend flight schools, and a memo related to Zacarias Moussaoui, were not called to the attention of senior FBI officials.
- Outside the Bureau, the FBI could not overcome bureaucratic rivalries to share information with other parts of the intelligence community.

When we prepared our recommendations, we considered whether or not to support the creation of a new domestic intelligence collection agency, or "MI-5" as the British model is called. We recognize that the United States is the only major democracy

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00305 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.246

that combines law enforcement and domestic intelligence at the national level. After much discussion, we decided against an MI-5 model. We decided it would be:

-- too risky to civil liberties;
-- take too long to set up;
-- cost too much money, and
-- sever the important link between the criminal and counterterrorism investigative work of the FBI.

Our consideration of this question also came at a time when significant reorganization – the creation of a Department of Homeland Security – was already underway. We did not want to overload the circuits,

We reviewed in detail Director Mueller's reforms since the 9/11 attacks. In our view, those reforms were moving in the right direction—and they still had a long way to go. In the end, we thought it was important to strengthen and institutionalize these reforms, not sidetrack them by creating a new entity.

We made recommendations for rebuilding the FBI into a world-class counterterrorism intelligence collection and prevention organization. We made the following recommendations for the FBI:

- Create an intelligence cadre—a specialized and integrated national security workforce—and make significant personnel reforms in recruitment, hiring, training and career advancement in order to develop this cadre;

- Ensure that this workforce is focused on the counterterrorism mission—and in particular, make sure that national priorities are being carried out in the field.

- Integrate analysts, agents, linguists and surveillance personnel in the field, so that a dedicated team approach is brought to bear on national security intelligence operations.

- Align the budget structure according to the Bureau's four main programs: (1) intelligence; (2) counterterrorism and counterintelligence; (3) criminal; and (4) criminal justice services – for better transparency; and

- Report regularly to Congress, in detail, on the qualifications of its analysts, and on the progress and ability of each field office to appropriately address FBI and national program priorities.

- We also made a critically- important recommendation to improve information sharing. We recommended that the President lead a government-wide effort to bring the major national security institutions into the information revolution and coordinate the resolution of legal, policy and technical issues across agencies to create a trusted information network.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00306 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.247

II. The Intelligence Reform and Terrorism Prevention Act of 2004

Congress responded favorably to our report, and stayed in session during the August recess. This Committee, and others, held hearings on our work. Congress spent the fall writing legislation. On December 17, President Bush signed into law the "Intelligence Reform and Terrorism Prevention Act of 2004," enacting several of our key recommendations.

The Act put into law our proposals regarding FBI reform:

- On an intelligence cadre, the Act requires that the FBI develop, train and reward a national intelligence workforce consisting of agents, analysts, linguists and surveillance specialists.

- On personnel reforms, the Act requires that the Bureau recruit and retain individuals with backgrounds in intelligence, international relations, language, technology, and other relevant skills. The Act also creates a career service for intelligence and allows for a reserve force to be created. It requires completion of intelligence community assignments and an advanced training course in order for agents to advance to higher level intelligence assignments.

- To focus the FBI on the counterterrorism mission, all agents must be trained in national intelligence matters, and they must be given meaningful national intelligence assignments.

- On a dedicated team approach, the Act requires that the FBI ensure that certified intelligence officers directly supervise each Field Office Group. Each Bureau Operational Manager at the Section Chief and Assistant Section Chief level must also be certified intelligence officers.

- On budgets, the Act requires the FBI to establish a budget structure that reflects the four principal missions of the FBI.

- On information sharing, the Act created the position of program manager for counterterrorism information sharing. That programmer manager has responsibility for ensuring better information sharing across and within the federal government, among state and local authorities, and also within the private sector.

- On information technology, the Act requires the FBI to maintain a state of the art and up to date information technology system.

- Finally, the Act sets reporting deadlines for the FBI to report to Congress on reform efforts.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00307 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.248

III. Reform to Date – Status Report

The provisions in the Intelligence Reform Act require Director Mueller to press forward with reform at the FBI. He faces formidable challenges. He needs to create a first-class domestic intelligence-gathering service, consistent with our laws and civil liberties, within the FBI. He needs to make the cultural and structural changes necessary to accomplish such a transformation.

- He needs to convert 56 field offices into fast moving, forward leaning centers focused on intelligence needed to spot terrorists and prevent future attacks. Prevention of terrorism, Mueller has said repeatedly, is now the FBI's top priority.

- He needs to hire and train new special agents and intelligence analysts with specialized knowledge and turn them into a dedicated intelligence workforce.

- He needs to create a better balance in information sharing. Everyone understands the "need to know" principle to protect information and save lives. The "need to share" principle is just as important if we are going to save lives.

How far has Director Mueller come in making these changes? He has offered his perspective this morning, and I find his perspective a valuable one. Let me offer some additional views.

National Academy of Public Administration. In January of 2005, when the National Academy of Public Administration delivered its report examining the progress of reform at the FBI, the panel declared that "substantial progress" had been made in transforming the Bureau into a strong domestic intelligence entity. The panel praised Director Mueller for taking major steps to integrate intelligence into the FBI's mission.

WMD Commission. Other reports have been more critical. In March 2005, the President's Commission on the Intelligence Capabilities of the Intelligence Community regarding Weapons of Mass Destruction, or WMD Commission, stated that the FBI's intelligence program was not fully integrated either within the Bureau or across the broader Intelligence Community. It found, for example, that the FBI has failed to give its new intelligence directorate control over intelligence operations in the field, and that unnecessary turf battles are being fought between the FBI and CIA.

The WMD Commission recommended creating a new National Security Service within the FBI, comprising both the Bureau's Counterterrorism and Counterintelligence Divisions and the Directorate of Intelligence. This recommendation has now been accepted by the President. The intelligence-related

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00308 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.249

aspects of the new Service, though not operations, come under the authority of the Director of National Intelligence.

Inspector General Report. In May 2005, the Department of Justice's Office of Inspector General updated its review of the FBI's counterterrorism intelligence analytical capability. Three years ago, it had reported that this capability was "broken," but now it finds both "significant progress" in hiring and training intelligence analysts. Yet according to the report, substantial problems remain:

- The FBI does not have a good sense of the number of analysts needed for its mission. The likelihood that analysts will "jump ship" and go to another agency has increased. 22% of the FBI's current intelligence analysts reported that they do not plan on staying with the Bureau as analysts beyond the next five years.

- Although newly hired analysts are well qualified, the FBI's intelligence analyst training is deficient in the areas of assessment and dissemination, and analysts are spending up to a third of their time on unrelated administrative work.

- Finally, the FBI still subordinates intelligence functions to investigative functions.

There is concern about the effects these problems may have on the FBI's efforts to build a well-qualified analytical corps. The Office of the Inspector General's report recommends that all FBI special agents undergo mandatory training on the role and capabilities of analysts, and that the analysts themselves need more extensive and rigorous training. The FBI says that these recommendations are already being implemented, and that in particular substantial funds are being devoted for training of counterterrorism special agents, analysts, and other personnel.

A. Information Sharing

Information sharing both within and outside the FBI has improved, but it is still not adequate.

Press reports from May of this year, for example, indicate that New Jersey officials and the New York Police Department are not sharing information with the FBI. They, in turn, believe they do not get the information they need from the FBI. There are reports of a rivalry between the FBI and the Department of Homeland Security, with the result that information is not shared between agencies or with local law enforcement.

Perhaps the most disturbing report on the progress of reform at the FBI has been the failure to install a new information technology system. Before 9/11, FBI field offices did not have compatible computer systems. Each division at

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00309 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.250

headquarters had its own system, making effective and rapid information sharing impossible. Director Mueller presented a comprehensive plan for remedying this deficiency. The FBI was authorized to spend $170 million on the third phase of a three-step technology overhaul known as the "Trilogy" project.

As of March 2005, the Bureau had spent $158 million of this money, a quarter of it on usable equipment and programs, and the rest on the "Virtual Case File." This is a program to link FBI field offices around the country, so that geographically-dispersed agents can share leads and collaborate on cases in real-time. The program, however, has proved unworkable and been scrapped.

The problem is not just that hundreds of millions of dollars appear to have been lost. Valuable time has been lost. Almost four years after the 9/11 attacks, the FBI still does not have a comprehensive workable system for sharing information.

It is appropriate to ask how long it will take to implement a new information technology system. According to Director Mueller, it may take 3 and a half more years to install one. It is appropriate to ask whether we can wait that long.

B. Leadership

The information technology setback at the FBI is indicative of a broader problem: there has been considerable turnover at the leadership level of the FBI over the last few years. The figures are disturbing:

- The average tenure of Senior Executive Service officers at the FBI is 13 months; none have served longer than Director Mueller.
- The median level of a special agent in charge is 15 months; only four have served longer than Director Mueller.
- Since 9/11, the FBI has had six different chiefs of its Counterterrorism Division.
- In the last two years there has been frequent changeover in the Bureau's top computer job.

This revolving door in management has to have serious consequences on the FBI's reform efforts.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00310 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.251

C. Summing Upon the Record on Reform

Overall, the record on reform at the FBI is mixed. Director Mueller believes that he has succeeded on some big issues. He has made substantial progress in making counterterrorism the FBI's number one priority, and directing this effort centrally from headquarters. He has sought to transform the FBI's culture. But the institution is proving resistant to change. At this point in time, we cannot say that Director Mueller has yet succeeded in creating a first-rate, modern, expert, and cohesive domestic security unit.

Progress has been made, but we need to ask whether it is enough. We should not underestimate the challenges facing Director Mueller. We should support his efforts to meet these challenges – but we also need to assess whether or not the progress made over the past four years warrants our continued confidence that the necessary changes *will* be made, and that they will be made soon enough.

But we do not have a limitless amount of time. The terrorists will not wait until our domestic security systems are fully reformed before attacking us where we are most vulnerable once again.

IV. Assessing the Future of Reform: What to Watch For

I believe there are several areas which we should watch carefully in order to assess just how far the FBI has come since 9/11 in order to determine whether we have come far enough.

A. Analysis

The collection of intelligence is not worth much if it is not adequately translated into realistic threat assessments. The FBI performed no such analysis of the threat to domestic security from terrorism before 9/11. Doing this job well must be a priority. We cannot decide what actions to take – we cannot set priorities on the application of resources – if we cannot assess the nature of the threat.

The Bureau needs to establish itself as a premier agency for analysis. In order to do this, it must give analytic capability the attention and respect that it deserves.

The 9/11 Public Discourse Project, on which I serve as a Board member, recently held a public forum covering the topic of FBI reform.

-- During this forum, long-term senior intelligence analyst John Gannon commented that at the FBI if you are not an agent you are "furniture."

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00311 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.252

-- He noted there is a lack of appreciation for analysts within the FBI that is reflected in inadequate resources being spent on developing and maintaining analytic expertise.

-- There need to be strong programs in place to recruit, train and evaluate analysts. Analysts need to see the commitment of FBI leadership to career paths for them that are attractive in terms of status and compensation.

-- Attrition rates for analysts – a chronic problem for the FBI – show some recent improvement. But we can and must do better.

B. Information sharing.

We must ensure that the FBI is sharing the right information with the right people in a timely fashion. The 9/11 Commission stressed the absolute importance of better intelligence sharing; the Intelligence Reform Act accepted these recommendations; the WMD Commission endorsed such provisions.

The Virtual Case File debacle has been discussed at length. The problem of information sharing is not just technical. The problem, in part, is also the nature of the FBI's mission.

In its counterterrorism efforts, the FBI combines both its conventional law enforcement role and its new preventative intelligence gathering role. One is designed to punish those who commit terrorist attacks, and seeks evidence that is legally admissible in court. The other is designed to prevent terrorist attacks before the fact, and seeks information to thwart planned attacks, regardless of whether it is legally admissible. This is one reason why cooperation between the FBI and the CIA, for example, was so problematic in the past.

The legal barriers that supported this separation of intelligence roles have now been eliminated. But institutional and cultural barriers to information sharing remain.

Breaking down these barriers is a high priority. You can change the law, you can change the technology, but you still need to motivate institutions and individuals to share information.

For this reason, Congress created the position of a program manager for counterterrorism information sharing across the federal government, and with state and local agencies, and as appropriate with the private sector. As of

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00312 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.253

today, this office exists, and a veteran intelligence expert fills the position. Yet he has no staff, funding, or other resources to do his job.

If we are to solve the information sharing problem at the FBI and elsewhere, it cannot be delegated down the line.

-- The success of information-sharing needs the personal attention and support of Director Mueller.

-- It needs the personal attention and support of the Director of National Intelligence.

-- It needs the personal attention of the President of the United States.

-- Standing in the way of information sharing is history, culture and the sheer inertia of government. You cannot overcome those barriers without the strongest possible support from the highest levels.

C. FBI management

For reform to succeed, we need to see greater stability in management responsibilities. We cannot afford to leave vitally important infrastructure projects up to the supervision of contract managers. As former Attorney General Thornburgh recently told us, flux at the leadership level simply compounds the difficulty of having Director Mueller be the focal point of all information coming through the system.

D. The National Security Service and Director of National Intelligence

The president has now mandated that the FBI will have a National Security Service. The creation of a new and special entity within the Bureau dedicated to gathering information on terrorists and preventing attacks should make permanent the reforms that were already underway and help ensure there is no backsliding.

The Director of National Intelligence has been given considerable authority over the new National Security Service within the FBI. Working out the specifics of what the DNI will be responsible for, and what the Director of the FBI will be responsible for in this new service, must be a priority.

We want stronger intelligence at the FBI, but not FBI operations under the control of intelligence. The guiding principle should be intelligence under the authority of the DNI, and operations under the authority of the FBI Director and Attorney-General.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00313 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.254

E. FBI relations with the CIA

The domestic and international intelligence divide between CIA and the FBI was a serious shortcoming before 9/11. According to FBI and CIA leadership, much progress has been made in cooperation. The CIA and FBI recently signed a memo of understanding outlining their respective roles inside the United States. The CIA also has provided significant numbers of analysts to help train FBI analysts and enhance the analytical capability of the FBI.

The relationship between the FBI and CIA must be seamless. We can no longer tolerate any failure to share databases on terrorists between agencies. For example, we have been working on the question of a unified terrorist watchlist for several years. We're not there yet. We need to get there.

F. The FBI's relationship with foreign domestic intelligence services

Information sharing with foreign security services is critical to defeating the terrorists. Director Mueller and Director Negroponte will need to ensure that exchanges of information are efficient and timely. As the FBI improves its analytic capability, and increases its knowledge of suspect individuals in the U.S. and overseas, it must have appropriate systems and rules in place for the effective sharing of this information with trusted allies. This will be an effective tool to help prevent the kind of attacks that occurred in London recently.

G. Setting priorities for State and Local law enforcement

As I mentioned earlier, if we do not have good analysis of the threat, we do not have the ability to set priorities for the use of our resources. The FBI must perform domestic threat assessments, and share these with state and local authorities. I hear complaints all the time that the federal government—in particular the FBI — is slow to share information, and does not communicate the nature of the threat. State and local law enforcement authorities do not know what to do, or where to put their resources.

The FBI chairs a number of joint terrorism task forces in major cities in the U.S. These standing committees bring federal, state and local capabilities to bear against the terrorist threat. The task forces are a good step toward ensuring cooperation at all levels of government. For them to be successful, the flow of information must not just be a one-way street from state and local authorities to the federal government. Success requires the FBI both to share information and involve state and local law enforcement authorities in joint operations.

Success also requires the FBI and DHS to coordinate a unified message to state and local authorities.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00314 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.255

H. Civil liberties

As the FBI becomes more deeply involved in gathering intelligence domestically, questions will inevitably arise about the impact its activities are having on civil liberties. Enhanced FBI intelligence collection is vital to the security of this nation, but so is a deep respect for our civil liberties.

Director Mueller and Director Negroponte's leadership will be critical here. They must insist loudly, clearly, by word and deed, on law enforcement, terrorism prevention, and the protection of civil liberties.

Congress must play an active role in oversight as the FBI's role expands. And the new Privacy and Civil Liberties Oversight Board must be vigilant as well.

V. Conclusion

When we issued our report a year ago, we stated the following:

> Our recommendation to leave counterterrorism intelligence collection in the United States with the FBI still depends on an assessment that the FBI—if it makes an all-out effort to institutionalize change—can do the job.

We stand by this statement still. Director Mueller is clearly making a strong effort to effect change. The obstacles are immense. We applaud the progress he has made so far; we urge him to forge ahead. We should give Director Mueller as much support as he needs to get the job done. We should be helpful and constructive.

The FBI has been reforming itself for four years. Everyone recognizes that there are still significant deficiencies in:

- the FBI's analytic capabilities;
- information sharing with other agencies and with local law enforcement; and
- information technology capabilities.

We still see bureaucratic rivalries between the FBI and other agencies.

It is fair to ask how long the FBI will take to reform itself.

Director Mueller's timeframe for effecting reform at the FBI is not infinite.

The United States has not been attacked at home since 9/11, yet we all understand that the threat of terrorism remains very real.

The threat to reform is also real. That threat is inertia and complacency. We need to maintain a sense of urgency to push reform efforts along as fast as possible.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00315 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.256

This Committee, and this Congress, need to continue to provide careful oversight of Director Mueller's reforms, and to provide to him your expert guidance. He needs your support for reform – and he and the FBI also need a strong push from the Congress and other friends of reform.

A strong and effective domestic intelligence function is not an option for the United States — it is an obligation. Our nation's security depends upon its success.

Thank you.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00316 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.257

Statement
United States Senate Committee on the Judiciary
FBI Oversight
July 27, 2005

The Honorable Patrick Leahy
United States Senator , Vermont

STATEMENT OF SENATOR PATRICK LEAHY,
RANKING MEMBER, COMMITTEE ON THE JUDICIARY
HEARING ON FBI OVERSIGHT
JULY 27, 2005

Mr. Chairman, thank you for convening today's important hearing on FBI oversight. This is a constructive opportunity to continue our efforts to remake the FBI into a modern domestic intelligence and law enforcement agency. Congress immediately rose to the post-9/11 challenges facing the Bureau by giving law enforcement agencies new tools, by funding information technology, and by pushing for key management and systemic changes at the Bureau. We have also had time to evaluate and adjust. Just last week, we unanimously passed out of the Committee the USA PATRIOT Act Reauthorization Bill, to extend law enforcement powers, while adjusting safeguards to address privacy and civil liberty concerns. Today, we have a panel of distinguished witnesses to help us evaluate the Bureau's progress, and I look forward to their input.

After 9/11, we all realized the FBI had a lot of work to do. The 9/11 Commission recommended crucial changes, such as creating an effective intelligence group, enhancing information sharing, improving linguistic capabilities, and addressing management concerns in hiring, training and advancement. The FBI has improved, as recognized by Inspector General Fine, members of the 9/11 Commission and others, such as the National Academy of Public Administration. But those evaluations also show substantial impediments to information sharing, effective use of analysts and expertise in domestic intelligence operations, and improving linguistic capabilities.

You, your leadership team and the hard-working men and women of the Bureau deserve the constant appreciation of all of us as Americans for all you do and for the sacrifices you make to do it. Especially after 9/11, the people of the FBI have invested untold overtime hours, working under great pressure, to handle the expanded duties that landed on the Bureau's doorstep that day. Constructive oversight is an invaluable partnership tool that can help the Bureau become as effective as the American people need it to be in thwarting terrorism and in its many other essential missions. And that is why you and we are here today.

Translators

I have followed the challenges faced by the FBI translation program for years and have tracked this effort closely since 9/11. Recognizing that the FBI would need to hire additional linguists with fluency in Middle Eastern, Central Asian and other languages and dialects, I added provisions to the original USA PATRIOT Act to facilitate the hiring of additional translators at the FBI.

Over the past year, the Office of Inspector General has issued two reports on the translation program. The first was a full audit and the other was the result of an investigation into the security of the operation after allegations of lax controls and possible espionage were leveled by a former contract linguist. I thank Mr. Fine and his staff for the significant effort they have made in this area, both to produce the reports and to ensure that public versions are made available in due course. These reports

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00317 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.258

have proven invaluable to those of us who believe vigorous oversight and government transparency are essential accountability tools in making the FBI as effective as the American people need the Bureau to be, and I hope these reports will be valuable to the Bureau in charting further improvements.

This morning the Inspector General released an update to his 2004 audit. He gives credit where credit is due and acknowledges that the FBI is making progress. We all recognize that it is extremely difficult, as a starting point, to find linguists who are skilled in languages uncommon in the United States. I recently spoke directly with Director Mueller about the translation program, among other oversight topics. I appreciate that the Bureau is working hard to address this challenge, but I remain troubled by the fact that it takes the Bureau, on average, 16 months to hire a contract linguist.

Numerous additional problems continue to plague the translation program. First, the number of hours of unreviewed counter-terrorism audio is increasing. Counter-terrorism recordings are as important as they sound; they include data gathered under foreign intelligence surveillance warrants. Even after the FBI adjusts the numbers to account for double counting, and after it consolidates data from field offices, the numbers still show a marked increase – from about 4,000 hours of unreviewed counter-terrorism audio recordings in April 2004, to more than 8,000 hours in March 2005.

Second, the amount of unreviewed counter-intelligence audio recordings remained somewhat constant, but the Inspector General found that field offices are still failing to review all of the high priority intelligence data within 24 hours.

Finally, with regard to quality control, new guidelines require a higher level of review and certification of translated material, but there apparently still is no nationwide system in place to implement these guidelines and monitor the quality of translations.

I want to see this program succeed. An efficient and versatile translation program is critical to the Bureau's ability to prevent terrorist attacks. We need to see more sustained progress in this area before we can be satisfied that the Bureau is meeting its responsibilities.

Information Sharing, Terrorist Screening Center, And Terrorist Watch Lists

A January 2005 report by the National Academy of Public Administration found that the FBI's information sharing practices, while improved, are largely ad hoc and lack mechanisms, such as penalties or incentives, to enforce or promote information sharing. That is a problem. Other weaknesses in the information sharing infrastructure are the current challenges with the Terrorist Screening Center and the Virtual Case File project.

After 9/11, there was broad agreement that the nation needed an accurate, reliable and comprehensive terrorist watchlist. The Terrorist Screening Center (TSC) was established in 2003 with the FBI as the lead agency, and it was charged with consolidating 12 terrorist watchlists. The consolidation has taken longer than anticipated, but the FBI has made notable progress. But as a recent report by Inspector General Fine shows, significant concerns remain. TSC's operations have been hampered by inadequate training, rapid turnover among the employees staffing at the 24-hour call center, and deficient information technology. And if a terrorist disaster struck, there are questions about whether TSC's continuity plans would provide sufficient redundancy to ensure access to the very information

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00318 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.259

that would be so critically needed at such a time.

The watchlists have also been plagued by inaccurate and incomplete entries. Names that should have been included in the list were not. Innocent individuals have been detained or prevented from airline travel due to list errors.

I am also concerned about whether the consolidated list is being used effectively. For example, the watchlist uses four risk-based handling codes to designate how law enforcement agencies should respond when encountering individuals on the list. A sample reviewed by the Inspector General showed that the majority of watchlist names – including nearly 32,000 individuals described as "armed and dangerous" – are designated for the lowest handling code, which does not require law enforcement encountering those individuals to contact the TSC or any other law enforcement agency. Some of these 32,000 individuals were also described as "having engaged in terrorism," "likely to engage in terrorism if they enter the Untied States," "hijacker," "hostage taker," and "user of explosive or firearms." It is unclear to me how individuals so described could be designated for the lowest handling. These designations raise significant concerns that law enforcement agencies may be caught unawares or may miss opportunities for updating TSC on the movements of such individuals.

There have also been repeated stories of plane diversions because terrorist suspects from the no-fly list have been allowed to board planes. If a person is so dangerous as to be on a no-fly list, then mid-flight is much too late to respond. Our screening processes must make sure that the list is effectively used to prevent the individuals from boarding planes in the first place.

Virtual Case File/Sentinel

It is no secret that many of us are greatly concerned about the FBI's handling of the Virtual Case File (VCF) project. The FBI bit off more than it could chew, failed to develop a finite and final list of project requirements, poorly chose to issue a contract without milestones and associated penalties, had inconsistent leadership, and lacked the capabilities and procedures necessary to manage the project well. As the Director knows from two appropriations subcommittee hearings, I found intolerable the fact that Congress – and this Committee in particular --- was not given the full story on how poorly the project was progressing until the entire project collapsed under its own weight. Taxpayers are out more $100 million, we have lost several crucial years in getting this essential task completed, and we have been told that the work product is not salvageable, with only "lessons learned" to show for this great expense.

I am also disturbed by recent reports from the General Accountability Office that an audit of the project has been substantially delayed by the FBI. Weeks go by before meetings are scheduled and GAO has had to wait several months, and in at least one case, as long as nine months, to receive requested documents. The Bureau has provided the wrong documents and has imposed other delays by requiring DOJ and FBI attorneys to screen documents before their release, and by limiting direct contact between the GAO and individuals involved in the project. Some of this sounds familiar to me. I have often been told that the FBI's answers to my questions are tied up in DOJ reviews. I hope that the FBI will make adjustments to reduce these delays. The GAO's audit will be critical as we move forward with the four-year replacement project – Sentinel ? and attempt to manage the already skyrocketing costs.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00319 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.280

While we are still waiting for the FBI to share with Congress the Sentinel cost estimates received quite some time ago, the numbers reported in the press are not encouraging. U.S. News & World Report reported it to be as much as $792 million, which would be several times larger than the amount previously dedicated to VCF -- $170 million – and more than the cost of the entire Trilogy project -- $581 million. The Bureau has disputed this figure, but it is hard to verify figures without access to the hard numbers. When I asked Director Mueller about the costs in a recent hearing, he suggested that he would rather discuss the issue in private, given procurement sensitivities. Director Mueller and I have met in private and those numbers were not forthcoming, but I hope that when the numbers are revealed, they are not in this expensive neighborhood. We remain very concerned about this project, we expect transparency and accountability, and there is no patience for another fiasco.

Counterintelligence and Counterterrorism

There are also other weaknesses in the Bureau's counterintelligence and counterterrorism efforts. The 9/11 Commission recently organized a series of panels as part of its Public Discourse Project to assess developments since its monumental report. Those discussions revealed that there are an insufficient number of intelligence analysts and significant weaknesses in programs to train and retain them. A former CIA intelligence officer pointed out that FBI culture continues to place a lower value on intelligence functions than investigative efforts, and that the Bureau inadequately invested in analysts' expertise or integrated them into positions of authority, influence and leadership.

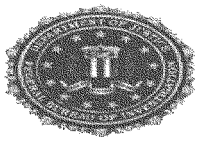
I am also concerned about reports that many top counterterrorism officials at the FBI do not have a detailed understanding or experience in counterterrorism. While other capabilities, such as leadership skills, are critical to the counterterrorism effort, I would also like to see a core competence in counterterrorism within the FBI's personnel resources. There appears to be some difficulty to filling counterterrorism posts. The discussions at the Public Discourse Project also reveal that the Bureau has 200 unfilled counterterrorism positions and is facing difficulty finding analysts and agents to fill those posts.

Conclusion

The FBI has undertaken a significant organization overhaul since 9/11. The times and threats have changed, and the Bureau has been adjusting in several key areas. The Bureau has made significant strides and I want to underscore and commend Director Mueller and the Bureau for that. But there is much work to do. I look forward to engaging our witnesses on how best to move forward.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00320 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.261



Statement
of
ROBERT S. MUELLER, III
Director
Federal Bureau of Investigation

Before The
United States Senate
Committee on the Judiciary

July 27, 2005

Good morning, Mr. Chairman, Senator Leahy, and Members of the Committee. I am pleased to appear before you today to update you on recent changes within the FBI and to address additional changes we anticipate in the near future. I would like to thank the Committee for your oversight of the FBI and your interest in ensuring our success in carrying out our mission.

I would like to take this opportunity before the Committee to discuss the President's recent announcement of the creation of an intelligence service within the FBI. This service will unify the FBI's Directorate of Intelligence, Counterterrorism Division, and Counterintelligence Division and will integrate FBI intelligence and investigative operations more fully into the broader Intelligence Community. Within this context, I would like to address three areas that directly impact the success of this new intelligence service: our Language Program, our Information Technology capabilities, and our ability to recruit, hire, train, and retain the expertise we need to build this service. Finally, Mr. Chairman, I would like to take this opportunity to reiterate the FBI's need for administrative subpoena authority in support of our efforts in the war on terrorism.

FBI Organization

Last month, the President announced that he had approved certain recommendations of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the WMD Commission). While the WMD Commission recognized that the FBI has made substantial progress in building our intelligence program, it expressed concern that our existing structure did not give the Director of National Intelligence (DNI) the ability to ensure that our intelligence functions are fully integrated into the Intelligence Community.

We are currently preparing a plan for implementing the President's directive to establish an intelligence service within the FBI. While the details of this plan are currently being discussed with the Department of Justice and the Office of the DNI, I would like to share with the Committee the broad concepts under which this service is being developed.

46051.262

One guiding principle of the FBI's intelligence program, as implemented by the Directorate of Intelligence, has been the integration of the FBI's intelligence and investigative missions. An FBI intelligence service will build on the progress of the Directorate of Intelligence and further promote this integration. The integration of our intelligence and investigative missions ensures that intelligence drives investigative operations. Further, this integration enables the FBI to capitalize on its established investigative capacity to collect information and to extend that strength to the analysis and production of intelligence. This intelligence service will integrate intelligence and investigative operations by combining our counterterrorism, counterintelligence and foreign intelligence investigative components with our intelligence component and by placing the service under the supervision of a single official who will report to the Deputy Director.

The development of a specialized national security workforce is a key component of this new service. We will develop this workforce through initiatives, many of which are already in place, designed to recruit, hire, train and retain investigative and intelligence professionals who have the skills necessary to the success of our national security programs. For example, in accordance with the Intelligence Reform Act, our Directorate of Intelligence has established a specialized and integrated national intelligence workforce, which consists of intelligence analysts, language analysts, and physical surveillance specialists, as well as 500 Special Agents. To support this workforce, we are developing an intelligence career service that addresses the full range of human resource issues from hiring to training to professional development and retention.

Finally, the creation of an intelligence service within the FBI will enhance our ability to coordinate our national security activities with the DNI and the rest of the Intelligence Community. The single FBI official in charge of the intelligence service will be able to ensure that we direct our national security resources in coordination with the DNI, who will have the authority to concur in the appointment of this official.

Mr. Chairman, this is a broad outline of our plans for an intelligence service within the FBI. I am happy to provide the Committee additional details as the implementation of this initiative progresses.

Directorate of Intelligence: Foreign Language Program (FLP)

Prior to September 11, 2001, translation capabilities, like most other FBI programs, were decentralized and managed in the field. Post 9/11, we established the Language Services Translation Center (LSTC) at FBI Headquarters to provide centralized management of the Foreign Language Program. The LSTC provides a command and control structure at FBI Headquarters to ensure that our translator resource base of over 1,300 translators, distributed across 52 field offices, is strategically aligned with priorities set by our operational divisions and

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00322 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.283

with national intelligence priorities.

We have now integrated Language Services into the Directorate of Intelligence. This integration fully aligns the FBI's foreign language and intelligence management activities and delivers a cross-cutting platform for future improvements across all program areas, including translation quality controls. We are also in the process of integrating linguists into our Field Intelligence Groups (FIGs) in each field office where their roles are expected to expand to include more intelligence reporting and analysis. Integration into the FIGs will establish a clear chain of command for the management and development of our language personnel. And, as their roles change, FBI linguists will receive greater training opportunities and Language Analysts will have greater promotion potential within the organization.

In addition, we have instituted prioritization processes to ensure that foreign language collection is translated in accordance with a clear list of priorities. The Foreign Language Program receives regular weekly updates to FISA prioritization. We are careful to ensure that the FBI's priorities are consistent with those set by the FISA prioritization board established by the Director of Central Intelligence. Our participation in this board has served to ensure our compliance in this area.

We also use a triage system to sift through collected materials. Once a document is received, a linguist quickly provides a cursory review and sets aside documents with pertinent information for future translation/summary. On audio lines that are mixed with several languages, a linguist reviews all the calls and forwards the foreign language sessions to the appropriate linguist for review and summary of pertinent sessions. We also route specific intelligence collection through the DI's English Monitoring Center (EMC) There, English Monitor/Analysts (EM) review the collection, summarize and report pertinent English materials, and forward the remaining foreign language items to the appropriate linguists across the country. This process allows our linguists to concentrate on the review, analysis, translation, and reporting of foreign language materials. On some audio FISA materials, where we are looking for a particular piece of information, a linguist will do a quick review and triage the audio for future translation.

With regard to the translation backlog, Mr. Chairman, we currently possess sufficient translation capability to promptly address all of our highest priority counterterrorism intelligence, generally within 24 hours. This prioritization and triage process has helped us reduce our accrued backlog. Of the several hundred thousand hours of audio materials and several million pages of text collected in connection with counterterrorism investigations over the last two years, only 1.8% of all audio (8,354 hours out of a total of 418,855 hours collected), 0.8% of all electronic data files (36,667 files out of 4,104,134 files collected), and less than 0.1% text (149 pages out of a total of 1,833,347 pages collected) exist as accrued backlog.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00323 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.264

Since the Office of the Inspector General completed its audit, we have reviewed more than 95% of all counterterrorism audio collected (403,864 hours out of a total of 426,593 collected). We found that 93% of the accrued backlog is attributable to either elongated "white noise" microphone recordings from certain techniques not expected to yield intelligence of tactically high value (4,668 hours of open microphone recording out of the total audio backlog of 8,354, or 56% of the backlog) or to audio from highly obscure languages and dialects that we are currently recruiting and hiring to address (3,362 hours due to a obscure languages out of the total audio backlog of 8,354, or 40% of the backlog).

We currently have translation capabilities in approximately 100 languages. The languages in the backlog are so rare that, in some cases, we have found that there is no one within the Intelligence Community with a proficiency in the language. We have addressed this issue through intense recruiting efforts, and have hired 9 additional linguists in one very rare language.

Mr. Chairman, I would also like to address some of the Inspector General's concerns about linguist hiring, vetting, and training. Since 9/11, we have recruited and processed more than 50,000 translator applicants. These efforts have resulted in the addition of 877 new Contract Linguists (net gain of 554 after attrition) and 112 new Language Analysts (net gain of 27 after attrition). The FBI has increased its overall number of linguists by 69%, with the number of linguists in certain high priority languages, such as Arabic, increasing by more than 200 percent.

At the same time, however, we must ensure translation security and quality. All FBI translator candidates are subject to a pre-employment vetting process that eliminates over 90% of those who apply.

There are currently over 3,000 FBI employees and contractors who have certified foreign language proficiency scores at or above Level II - basic working proficiency - including 406 Language Analysts and 959 Contract Linguists.

More than 95% of the FBI's linguists are native speakers of their foreign language and hold Top Secret security clearances. Their native-level fluencies and long-term immersions within a foreign culture ensure not only a firm grasp of colloquial and idiomatic speech, but also of heavily nuanced language containing religious, cultural, and historical references. Beyond these qualities, over 80% of FBI linguists hold at least a bachelor's degree and 37% hold a graduate-level degree. These qualities make them extremely valuable to the FBI's intelligence program, but also particularly attractive to other employers seeking these scarce skill sets. Strong demand for their language skills from other government agencies and the private sector is well documented. It is due in large part to this demand and competition that annual attrition among FBI Language Analysts has risen to approximately 7% since 9/11. Our attrition rate for contract

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00324 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.265

linguists is approximately 11%.

We are also working to increase the language proficiency of other FBI employees. We have made added investments to our language training and cultural awareness programs. Last year alone, our Foreign Language Training Program provided training and/or self-study materials to 1,470 FBI employees in 32 languages.

The FBI meets the need for Special Agent linguists by hiring agents who already have language skills, and also by offering agents training in critical foreign languages. Special Agents are proficient in 45 foreign languages, and there are currently 1,340 Special Agents who have Level 2 foreign language proficiency, including 35 Agents who speak Arabic. The Language Training Program component of the DI's Training and Oversight Unit provides high-quality, cost effective foreign language and language-related training to Special Agents whose jobs require them to use foreign languages, work with non-Roman alphabets, or have an understanding of foreign cultures.

The FBI Directorate of Intelligence manages the Special Agent Linguist Program and the language training that supports agent linguist requirements. The Special Agent Linguist Program assesses the deployment of Special Agents who are proficient in a foreign language and recommends permanent and temporary placement of new and experienced agents with foreign language proficiency in response to the FBI's investigative and intelligence priorities. Special Agents proficient in foreign languages are assigned to field offices, legal attaches, FBI Headquarters and the FBI Academy.

We have also taken steps to ensure proper security and continuing quality from the linguists we bring onboard. We have instituted a post-adjudication risk management program that mandates periodic personnel security interviews, polygraph examinations, and database access audits for each FBI translator. In the event this process discloses questionable or inappropriate associations based on self-reporting, or if such associations are brought to our attention by a third party, a security assessment is immediately conducted by the appropriate field office squad in coordination with our Security Division. Whenever credible and serious allegations surface, the translator's access to FBI space and information is suspended.

While we share the OIG's concerns regarding our quality control procedures, we are strengthening them by instituting national Translation Quality Control (QC) Policy and Guidelines. The FBI's QC Program requires that, after an initial week of intense training, all work performed by new linguists during their first 40 hours of service is subject to review by a senior linguist. Work performed during the second 80 hours of service will also be heavily spot-checked, and later checked with decreasing frequency as required. In all, it is estimated that each new linguist hired or contracted by the FBI will require an investment of at least 120 hours by a senior linguist dedicated to QC.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00325 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.286

Mr. Chairman, we recognize that the FBI's foreign language program is key to the success of both the FBI's intelligence and law enforcement missions. We appreciate the oversight by this Committee and by the OIG and look forward to working with you in ensuring that we have the translation capabilities we need to address the many threats we face as a nation.

FBI Information Technology

Mr. Chairman, we recognize that the ability to assemble, analyze, and disseminate information both internally and with other intelligence and law enforcement agencies is essential to our success in the war on terrorism. As a result, we have made modernization of our Information Technology (IT) a priority and have developed a coordinated, strategic approach to IT under the centralized leadership of the Office of the Chief Information Officer (OCIO).

The OCIO has developed a Strategic IT Plan, a baseline Enterprise Architecture, and a system for managing IT projects at each stage of their "life cycle" from planning and investment, through development and deployment, operation and maintenance, and disposal. In addition, the OCIO has been working closely with the OIG to address its recommendations for achieving our IT goals. We have made substantial progress in each of these areas:

- The need for a sound program management structure
- The need for establishment and enforcement of appropriate processes
- The need for Life Cycle Management controls and process
- The need for an empowered Chief Information Officer
- The need for Portfolio Management and Investment Management
- The need for an Enterprise Architecture
- The need for a Strategic Information Technology Plan

The modernization of our IT capabilities will be completed in the form of a Service-Oriented-Architecture (SOA). "Sentinel" will be one such service, or, more accurately, a suite of services geared to evolve with our new and emerging needs, to work within and take advantage of the infrastructure, equipment and networking improvements effected by the Trilogy Program. The Trilogy Program was planned as a modernization effort for system infrastructure, network optimization, and upgrade or replacement of the five most important FBI investigative applications supporting the field. At the same time, as these efforts got underway, current events radically changed the mission focus and, consequently, the information to support the new focus. This resulted in new and emerging requirements, including the need for better collaboration, complex workflow analysis and tracking programs, and a critical need for information sharing.

Sentinel is not the Virtual Case File (VCF) which, as we know, suffered from inadequate management control, new and changing requirements, and the inability to maintain pace with

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00326 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.267

these technical requirements. Sentinel differs from VCF in that it will serve as the platform from which services can be gradually deployed, each deployment offering added improvements. Sentinel will pave the road, starting with our legacy case management system, for subsequent transformation of all legacy applications to modern technology under our Enterprise Architecture. Services to be provided by Sentinel are currently planned for deployment in four phases, each phase providing standalone capabilities, each incrementally developed and deployed. In this manner, as each phase is developed, lessons learned from earlier deployments can be leveraged to our advantage. Early next year, initial development will begin; the full deployment of all services supporting our information management needs is anticipated to take a little over 40 months.

Mr. Chairman, I am aware that the Committee is interested in the estimated total cost of the Sentinel program. At this time, cost estimates are considered "source selection information" as defined by the Federal Acquisition Regulation, meaning that any public disclosure might improperly affect the bidding process. The FBI is committed to obtaining the best product at the lowest cost to the American people and we do not want to prematurely disclose information which may influence bids from potential contractors.

Human Resources

The men and women of the FBI are our most valuable asset. In order to continue to recruit, hire, train, and retain quality individuals for our expanding human capital needs, we have undertaken a re-engineering of our human resource program.

- We have retained the services of an outside consulting firm to review of business processes for selection and hiring, training and development, performance management, Intelligence Officer certification, retention, and career progression.

- We have removed non-human resource functions, such as facilities management, from the Administrative Services Division to create a pure human resource function.

- We have hired an executive search firm to identify a Chief Human Resources Officer for the FBI with significant experience in transformation of HR processes in a large organization.

- We have made substantial progress in building a specialized and integrated Intelligence Career Service comprised of Intelligence Analysts, Language Analysts, Physical Surveillance Specialists, and Special Agents.

- We have developed a Special Agent career path that will be implemented in

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00327 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.288

October 2005. These career paths will take into account the background and experience of the Agent in determining the Agent's future career path in one of five programs: Counterterrorism, Counterintelligence, Intelligence, Cyber, or Criminal. This policy will promote the FBI's interest in developing a cadre of Special Agents with subject matter expertise.

These are just a few of the initiatives underway to improve the FBI's human capital and to ensure that we develop a workforce that is prepared to meet the challenges of the future.

Administrative Subpoenas

Mr. Chairman, when I last appeared before the Committee, my prepared testimony included a request for administrative subpoena authority in support of our counterterrorism efforts. I was remiss in not including that request in my oral remarks and would like to take the opportunity to do so at this time.

As you know, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

Instead, we rely on National Security Letters (NSLs) and FISA orders for business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and enforcement is difficult because the request is in the form of a letter, not a subpoena or court order. FISA business record requests, although delivered in the form of a court order, require the submission of an application for an order to the FISA Court. This is a time-consuming process and, in investigations where there is a need to obtain information expeditiously, a FISA order for business records, which does not contain an emergency provision, may not be the most effective process to undertake.

As a result, we submit that the administrative subpoena would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs and it would provide the expediency not available with a FISA business records order. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal would provide the recipient the ability to quash the subpoena on the same grounds as a grand jury subpoena.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00328 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.289

Conclusion

Mr. Chairman and Members of the Committee, thank you again for this opportunity to discuss these important issues concerning the transformation of the FBI. Much has been accomplished. Much remains to be done. But our strategic plan, our methodology and process improvements are guiding our prioritization and performance in support of the FBI mission.

I am happy to answer any questions you may have.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00329 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.270

UNCLASSIFIED

STATEMENT FOR THE RECORD BY PROGRAM MANAGER FOR THE INFORMATION SHARING ENVIRONMENT JOHN A. RUSSACK BEFORE THE SENATE JUDICIARY COMMITTEE

PANEL DISCUSSION ON FBI OVERSIGHT July 27, 2005

INTRODUCTION

Over the last year, both the executive and legislative branches of government have responded to the recommendations of the 9/11 and WMD commissions to improve information sharing while protecting the freedom, information privacy, and other legal rights of Americans. Last August the President issued Executive Order 13356 to ensure that terrorism information is shared broadly among federal agencies; state, local, and tribal governments; and the private sector. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 devotes an entire section to this issue. So, while the institutional foundations are now in place to allow us to make significant progress in the way we share terrorism information, there are still a number of hurdles that exist that will require time and hard work to surmount. The administration is committed to identifying and removing all impediments that prevent us from providing the necessary information to those who need it, when they need it.

In my statement today, Mr. Chairman, I first want to briefly describe the specific role of the Program Manager in implementing the Information Sharing Environment (ISE). I will then highlight the major issues I believe must be addressed to achieve more open and transparent access to terrorism information as envisioned by both the 9/11 and WMD commissions.

ROLE OF THE PROGRAM MANAGER

The IRTPA Act defines the Information Sharing Environment as the combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of Federal, State, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration among users to combat terrorism more effectively. It requires the President to designate an individual to serve for a two-year period as the program manager (PM) responsible for information sharing across the federal government. The PM's duties include:

- Planning and overseeing the implementation of, and managing the Environment;
- Assisting in the development of policies, procedures, guidelines, rules, and standards as appropriate to foster the development and proper operation of the Environment; and

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00330 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.271

- Supporting, monitoring, and assessing the implementation of the Environment by federal departments and agencies, and regularly reporting the findings to Congress and the President.

In April, I was designated by the President to be the PM. In June, the President directed that the PM be part of the Office of the Director of National Intelligence (ODNI). Although I report to the DNI, the mandate is broad, covering access to terrorism information across federal, state, local and tribal governments and the private sector. We are now working to define specific objectives in support of the direction in the IRTPA, develop a work plan, organize the staff, and fill key leadership positions with experienced people from a variety of backgrounds. FBI expertise will be an essential element of the PM's knowledge base.

MAJOR ISSUES IN INFORMATION SHARING

On June 15, we submitted the PM's first deliverable to the President and the Congress. This preliminary report identified five broad issues that define the agenda for the Program Manager's office over its two-year life. The first of these is that existing authorities, policies, and procedures governing roles and responsibilities can be ambiguous and conflicting. Because information protection standards vary, decisions on reconciling the need to protect information with the need to share information are applied inconsistently, contributing to information segregation rather than integration. The PM, in consultation with the Information Sharing Council (ISC), will review these conflicting policies and develop actions to clarify the roles and authorities of participating agencies. With respect to the FBI, the policies relating to sharing of information between law enforcement and the intelligence community have been reviewed and commented on extensively already. I will make sure that existing policies fully reflect the current state of the law, so that information sharing is as robust as legally permitted, consistent with the need to protect privacy and civil liberties.

The second issue—trust between organizations—has been identified by a number of experts as a barrier to effective sharing. Organizations are often reluctant to share information because they believe that the recipients may misunderstand or misapply it. They perceive that the risks of sharing outweigh the advantages. Fostering trust across all organizations is a formidable challenge. Training and education, collaborative processes, personnel exchanges, and greater managerial accountability are all important factors in achieving the level of trust we need to win the war on terrorism. Increased trust should be a natural outcome of participation by all key stakeholders in the establishment and operation of the Information Sharing Environment. Trust plays a particularly important role in sharing between the law enforcement and intelligence communities, which have historically had distinct missions, cultures and rules. Now that the USA PATRIOT Act has effectively removed the historical "wall" between criminal investigations and intelligence officials greater information is legally permissible. My office will need to pay close attention to fostering trust in the relationships between these communities.

The third issue concerns the inability of some or all users to access the information they need because of controls imposed by the originating organization. The need-to-know principle, that has influenced information sharing decisions since the early days of the Cold War, can no longer be the exclusive criterion for such decisions in the era of the War on Terror. Moving to an Information Sharing Environment will necessitate shifting the paradigm to find the

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00331 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.272

appropriate balance between the need-to-know and the need-to-share, but will still require rigorous safeguards to ensure protection of national security and civil liberties. The PM's office will work with the Information Security Oversight Office and others to develop the policies and procedures required to achieve this fundamental change in thinking, recognizing, of course, that some access controls may be required by applicable laws or are otherwise necessary for protecting privacy and civil liberties.

The fourth issue is one that has been highlighted by both the 9/11 and the WMD commissions, the Markle Foundation, and others. That is that improved information sharing can only be achieved in parallel with the protection of the information privacy and other rights of Americans. In response to the IRTPA, a Privacy and Civil Liberties Oversight Board is in the process of being established to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism. The Information Sharing Council, established by the IRTPA, will work in conjunction with this Board to address the need to protect privacy and civil liberties in the Information Sharing Environment. My office will be especially sensitive to privacy and civil liberty concerns relating to information sharing with the FBI given the nature of the information it lawfully collects.

Lastly, the preliminary report identified the need to remove any technological barriers to information sharing. In large measure, the technology needed to improve interoperability and information sharing is available today; it should be viewed as an enabler rather than a barrier. On the other hand, disagreements over roles and responsibilities coupled with inadequate or outdated policies, procedures, and standards often impede our ability to use available technology effectively. A number of experts have commented on the vast and confusing array of systems, databases, networks and tools that users must deal with. In most cases, however, this vast and confusing array is caused not by technological barriers, but by policies, protocols, and overly zealous security regulations. These and any other barriers must be stripped away so that technology can be used to its greatest advantage.

SUMMARY

Mr. Chairman, I appreciate the opportunity to provide the committee with a brief update on the activities of the Program Manager's Office, which is still in the early stages of being organized and staffed. My goals, for my two-year term, are to develop and coordinate an architecture and plan for implementing the ISE, and put performance goals and metrics in place so that we can measure our progress. I will be glad to discuss any specific concerns during the Question and Answer part of this session. Thank you.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00332 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.273

TESTIMONY BEFORE THE

FBI OVERSIGHT HEARING OF THE

SENATE COMMITTEE ON THE JUDICIARY

Washington, D.C.

July 27, 2005

By

William H. Webster

46051.274

Chairman Spector, Senator Leahy and Members of the Committee,

Thank you for the privilege of appearing before you this morning to discuss generally the role of the FBI in collecting, assessing, data mining and sharing intelligence of interest to the many agencies, federal, state and local, who have been waging the battle against terrorism especially since the tragedy of 9/11 almost four years ago.

While the emphasis is on an examination of progress made since 9/11, I think some reminders of an earlier period are in order in order to add context to what has become the FBI response to terrorism.

I took office as Director of the Federal Bureau of Investigation in February 1978 in the wake of the investigations which lead to the Church and Pike Committee Reports. When I called on Vice President Mondale as a new Director, he presented me with copies of both Reports and admonished me to read them carefully. These reports contained strong recommendations against the CIA engaging in activities inside the United States and discouraged the FBI from engaging in operational activities abroad. The predominant restrictions related to "need to know". In the 14 years that I served first as the Director of the FBI and then as Director of Central Intelligence, the guidance that we receive from the Department of Justice and our own legal counsel was strongly influenced by those two Congressional documents. A reasonable short hand would be "stay away from

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00334 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.275

each other". Beware of using evidence developed through intelligence sources in criminal investigations.

But of course there were exceptions and important cooperation did occur in the world wide struggle against terrorism. In 1987, a notorious terrorist, Fawaz Younis, was located in Cyprus after he had left his Sudanese sanctuary. The CIA managed to lure him into open waters where a U.S. naval vessel was waiting just over the horizon. The arrest was effected by FBI special agents and he was brought to the United States where he was tried and convicted. There are other examples of course but they were largely overseas.

In 1987, when I was Director of Central Intelligence, I signed a Memorandum of Understanding with the Director of the FBI following the Edward Howard investigation in which the CIA agreed to notify the FBI promptly whenever one of its employees became a suspect on national security issues.

The adoption of the Patriot Act following the 9/11 tragedy shifted the emphasis to "need to share". It was like a large ship changing course against the tides of Church and Pike. Getting the word out, and understood, was doable but not an easy task. Moreover, the archaic condition of the Bureau's electronic case management system, designed during the Church-Pike Committee days, did not lend itself readily to tasking from other agencies of the intelligence community. Efforts to patch what is now a 14 year old mainframe had been both expensive and

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00335 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.276

frustrating. I put this right at the top of problems affecting information sharing by the FBI with other agencies. When I chaired a special commission to examine the internal security provisions of the FBI in the wake of the arrest and conviction of Robert Hanssen in 2001, we filed four classified appendices to our report relating to these computer deficiencies. I believe that more than patchwork, however expensive, is absolutely required so that the FBI can fulfill it's mandate of sharing the vast amounts of intelligence which can be mined from its stored data.

Although I have seen reports to the contrary, I believe that it is unfair to attribute problems in information sharing to cultural attitudes. I believe they were more rightly attributed to the understandings that flowed from the Church and Pike Committee Reports and were underscored and supported by departmental guidance and Congressional opposition to domestic intelligence sharing. In my nine years at the FBI, I found the men and women ready to respond to new directions that did not embroil them in unfair charges or put their careers at risk. The various joint projects, such as counterterrorist centers, brought the CIA and FBI closer together in a common cause.

Still, "need to share" is not a total substitute for "need to know". Sources and methods must be protected and honored if law enforcement and intelligence agencies are to be effective in recruiting and utilizing information obtained at great risk from such sources. There also continues to exist the problem

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00336 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.277

of the "third agency rule" under which the FBI, or the CIA, receives sensitive information from an intelligence agency of another country on condition that it not be shared outside the agency to whom it is given.

I currently serve as Vice Chairman of the Advisory Council on Homeland Security, an organization established by President Bush shortly after the 9/11 tragedy. With the creation of the Department of Homeland Security, we have been directed to work closely with the Secretary of Homeland Security. One of the challenges is to make important, sensitive information available to the DHS and at the same time honor the "need to know" principle. There may be as many as 100,000 first responder agencies -- police departments, fire departments, etc. who are most likely to be first on the scene and also may be best situated to prevent a terrorist event if they have the needed information. Homeland Security is entitled to and does receive intelligence from the CIA, the FBI and other members of the intelligence community. First responders rarely need to know the sources of the information or the methods by which the information was obtained. I believe it is sufficient to supply these agencies promptly with "finished intelligence" which sets forth the information without disclosing sources or methods. There may be exceptions but this should certainly be the basic principle if sensitive sources are to be protected.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00337 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.278

In 1978, when I took office, the three top priorities of the FBI were: organized crime, white collar crime and foreign counterintelligence. In 1980, I added terrorism to that list. We had been experiencing approximately 100 terrorist incidents a year, certainly not of the dimension of the attack on the World Trade Center, but life-threatening, lethal and a danger to our society. Within the FBI we focused on "getting there before the bomb went off". Prevention and interdiction obviously depended upon much better intelligence than we had had in the past. We worked on this, developed our sources, worked effective undercover operations and acted preemptively when appropriate. By the time I moved to the CIA in 1987, we were down to 5 or 6 terrorist events a year, and the year following there were none. I attribute this to highly skilled, dedicated, professional law enforcement and especially to better intelligence, along with cooperation from friendly agencies in Canada and other parts of the world.

We have made substantial progress in coming to grips with even larger terrorist activity and plotting in the past few years. Intelligence is the key. Without it, the terrorist is likely to succeed in his terrorist activity, leaving it to law enforcement to track him down and prosecute him. Prevention requires intelligence.

In summary, I believe that the FBI has significantly transformed itself to meet the current threats. It probably needs to improve its analytical capability,

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00338 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.279

which historically has been underdeveloped. Translators are badly needed to keep up with processing signals intelligence, documents and other important information. The biggest challenge, in my view, is to confront, in a rational way, the consequences of an archaic electronic data system that preceded the Patriot Act and would be considered obsolete by any modern enterprise. It needs a search engine which can be navigated with much greater speed and with more precision in locating those dots that were not found when they were needed.

Many forensic improvements, for which the FBI deserves great credit, are making it increasingly effective in this war on terrorism. DNA evidence, computerization of fingerprints, psychological profiling and other scientific techniques have proved their value. These efforts should be supported and properly funded. It makes no sense to have the best trained special agents in the world if they are not properly equipped and guided by the best available information. Sir William Stephenson, the famous "man called Intrepid", once wrote about the importance of gathering intelligence and managing the process. He concluded "in the integrity of that guardianship lies the hope of free people to endure and prevail".

When we talk about guardianship there is also the matter of oversight. The special commission on 9/11 strongly recommended that the Congress streamline its oversight procedures. This has not happened. It is my understanding

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00339 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.280

that there are some 88 Congressional Committees that claim oversight responsibility in the Department of Homeland Security. This needs to be addressed.

We now have a new organization of the intelligence community and a new leader. While the 200 page Act covers many of the issues, the key authorities of the Director of National Intelligence -- were not as expressly granted as I would have liked, but I believe Director Negroponte will assert them fully as needed. Of paramount importance is his responsibility to insist upon the level of cooperation and sharing among the members of the intelligence community that I believe the President and Congress intended in this reorganization, and that it be done with appropriate protection of sources and methods so essential to our national security.

VerDate Aug 31 2005 09:37 Jan 08, 2009 Jkt 045063 PO 00000 Frm 00340 Fmt 6633 Sfmt 6011 S:\GPO\HEARINGS\46051.TXT SJUD1 PsN: CMORC

46051.281