AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–706

FBI OVERSIGHT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MAY 2, 2006

Serial No. J–109–72

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

31–268 PDF WASHINGTON : 2006

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

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

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

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Grassley, Hon. Charles E., a U.S. Senator from the State of Iowa, prepared statement	269
Kennedy, Hon. Edward M., a U.S. Senator from the State of Massachusetts	2
prepared statement	274
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	12
prepared statement	275
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania	1

WITNESSES

Calbom, Linda M., Director, Financial Management and Assurance, U.S. Government Accountability Office, Washington, D.C.	39
Fine, Glenn A., Inspector General, U.S. Department of Justice, Washington D.C.	37
Gannon, John C., Vice President for Global Analysis, BAE Systems Information Technology, and Former Staff Director, Homeland Security Committee, U.S. House of Representatives, McLean, Virginia	40
Mueller, Robert S., III, Director, Federal Bureau of Investigation, U.S. Department of Justice, Washington, D.C.	4

QUESTIONS AND ANSWERS

Responses of Linda M. Calbom to questions submitted by Senator Specter	48
Responses of Glenn A. Fine to questions submitted by Senators Specter, Grassley, and Schumer	53
Responses of John C. Gannon to questions submitted by Senator Specter	60
Responses of Robert S. Mueller to questions submitted by Senators Specter, Leahy, Grassley, Kennedy, Kyl, DeWine, Feingold, Schumer, Durbin, and Feinstein	65

SUBMISSIONS FOR THE RECORD

Calbom, Linda M., Director, Financial Management and Assurance, U.S. Government Accountability Office, Washington, D.C., prepared statement and attachments	212
Department of Justice, Federal Bureau of Investigation, memoranda	230
Fine, Glenn A., Inspector General, U.S. Department of Justice, Washington D.C., prepared statement	234
Gannon, John C., Vice President for Global Analysis, BAE Systems Information Technology, and Former Staff Director, Homeland Security Committee, U.S. House of Representatives, McLean, Virginia, prepared statement	254
Mueller, Robert S., III, Director, Federal Bureau of Investigation, U.S. Department of Justice, Washington, D.C.	279
New York Times, April 19, 2006, editorial	285
Plan Dealer, Cleveland, Ohio, April 29, 2006, editorial	287
Seattle Post-Intelligencer, March 21, 2006, article	288
U.S. News & World Report, April 17, 2006, article	290
Washington Post, April 19, 2006, article	292

FBI OVERSIGHT

TUESDAY, MAY 2, 2006

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, Kyl, DeWine, Sessions, Cornyn, Leahy, Kennedy, Feinstein, Feingold, Schumer, and Durbin.

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

Chairman SPECTER. Good morning, ladies and gentlemen. The Judiciary Committee will now proceed with the oversight hearing on the Federal Bureau of Investigation, and we welcome the distinguished Director, Robert Mueller.

The FBI, with its great tradition for law enforcement and investigative techniques, has enormous responsibilities in an era where we are fighting terrorism, and it has great responsibilities in the protection of civil liberties as well; a delicate balance which the United States has been so adept at maintaining. The FBI is being very seriously challenged this year and the years intervening since 9/11/2001 and will be challenged into the future.

The Federal Bureau of Investigation has responded with very significant technological changes, and we will be taking a look at those today. We have been in touch with the Director on an informal basis to review what he has done with the so-called Virtual Case File, which had a cost in the range of $170 million, and what is being done now with the very extensive $305 million contract to Lockheed Martin.

A GAO report in February of this year has raised some very serious questions as to the adequacy of the FBI's control over the Trilogy project; GAO reported that there were payments of unallowable and questionable contractor costs and missing assets. We will be looking into the very important issue of information sharing, which was a major problem with the agencies prior to 9/11 and one which we have tried to correct with the creation of a new Directorate, which is a subject of ongoing concern.

A March 2006 GAO report found that there are still very substantial issues relating to information sharing. We will be asking the Director about that.

In the war on terror, there are still grave difficulties. The FBI statistics disclose a translation program as taking 14 months to secure contract linguists. A 2005 March report by the Department of Justice Inspector General found that there were more than 8,000 hours of counterterrorism audio that had not been reviewed. The 2005 Office of the Inspector General report raised questions about whether there was adequate coverage on the identities of people who constituted threats.

We are also going to be inquiring today on the recent FBI action looking to obtain some of the files of the late columnist Jack Anderson. A question as to why now. If those files were important, why not have sought their return during Jack Anderson's life, and would if be more appropriate to have a judicial action in replevin, for example, as opposed to, as reports have it—and we want to find out from the Director—having two agents appear in the home of the custodian of those records?

Another issue of very substantial concern is what is happening with the investigation of journalists. This Committee is about to report out a bill on reporter's privilege triggered by the 85 days of incarceration of Judith Miller. No doubt national security interests are of enormous concern, and there is an issue as to whether that kind of a contempt citation is appropriate where the focus has shifted from national security, shifted from the disclosure of the identity of a CIA agent, to whether people are telling the truth before a grand jury. That is a serious matter as well, but not one which rises to the same level as national security.

There has been recent speculation as to whether two criminal statutes relating to the disclosure of classified information may be used to prosecute reporters. A very extensive story appeared in the Sunday Times, which referred back to the Pentagon Papers case. The issue has been lurking for a long time on the concurring opinions of Justice White and Justice Potter Stewart, where Justice White says, "I would have no difficulty in sustaining convictions under these statutes on facts that would not justify the intervention of equity and the imposition of prior restraint." The Pentagon Papers case involved the effort to restrain the Times from publishing, and the White-Stewart opinions state pretty flat out that there is authority under those statutes to prosecute a newspaper, to inferentially prosecute reporters. And if that is so, that is something which requires some oversight and some analysis by this Committee, going back to the formulation of those statutes and to what Congressional intent was at that time, and depending upon the administration's interpretation of the statutes, whether there needs to be some further action by the Congress on modification or clarification of those statutes.

Senator Leahy will be along shortly, Mr. Director. In his absence, Senator Kennedy, would you care to make an opening statement?

STATEMENT OF HON. EDWARD M. KENNEDY, A U.S. SENATOR FROM THE STATE OF MASSACHUSETTS

Senator KENNEDY. Just a brief one, if I could. Mr. Chairman, we want to welcome Mr. Mueller, and thank you.

No challenge that we face is more important than dealing effectively with the terrorist threat facing the Nation and reform of the

FBI as an essential part of meeting that challenge. We all agree on the need for strong powers for law enforcement and intelligence offices to investigate terrorism and prevent future attacks and improve information sharing between Federal, State, and local enforcement. And in the wake of the tragic events of September 11th, Congress, the administration, and the country face the urgent need to do everything possible to strengthen our National security and our counterterrorist efforts.

On 9/11, we were united in our commitment to protect our country, to respond aggressively to terrorism and destroy al Qaeda. This was not an issue of party or partisan politics. We all worked together.

Unfortunately, however, we are now at an impasse where the administration refuses to work with Congress, and it is putting our national security and the public trust at risk. There is a way to fight terrorism within the framework of our Constitution. As Supreme Court Justice Robert Jackson wrote in 1941, "The Constitution is not a suicide pact."

Thirty years ago, when the cold war threatened our security, a Republican administration and a Democratic Congress worked together to pass the Foreign Intelligence Surveillance Act, giving broad authority to the Government in cases involving national security. Then, as now, the debate was driven by reports of watchlists, sweeping surveillance programs. Then, as now, the American people had questions about the proper scope of the President's authority.

Today, the politics of fear seems to be driving our National security policy, and at the same time, there are fundamental questions about whether we are getting it right. And there are new concerns that we may not be any safer now than we were 4 years ago. So I hope that you can address some of the concerns about the job the FBI is doing to get its house in order and to help us meet the national terror threat.

Thank you, Mr. Chairman.

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

Chairman SPECTER. Thank you very much, Senator Kennedy.

Director Mueller comes to the Office of the Director of the FBI with an outstanding record. He was an Assistant Attorney General in the Criminal Division of the Department of Justice. He was the United States Attorney for the Northern District of California, San Francisco, and also the United States Attorney for the District of Massachusetts, and after holding those lofty positions, came back to the criminal courts of Washington, D.C., to try cases—perhaps the highest calling, certainly higher than that of a Senator, and maybe even higher than that of a Director of the FBI.

It is our practice on these oversight hearings, Director Mueller, to ask you to be sworn in, so if you would stand. Do you swear that the testimony you will give before the Judiciary Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Director MUELLER. I do.

Chairman SPECTER. We will turn off the time clock for Director Mueller. We will keep it on for the Senators on the 5-minute

rounds, but take the time you need, Mr. Director, to make 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, members of the Committee, for having me here today. I am pleased to appear before you to thank you, first of all, for your continued work with the Bureau. I appreciate your efforts to ensure our success as we pursue the shared goal of making America safer, as well as preserving our civil liberties.

As this Committee knows, much of the last year has been devoted to a national discussion about the tools that should be afforded to the men and women engaged in the fight against terrorism, both at home and abroad. And I do want to thank this Committee and the Chairman for your work in producing what I consider to be a balanced law reauthorizing the USA PATRIOT Act. Through your efforts, our agents will retain the tools necessary to wage an effective fight against terrorism, within a framework that ensures important safeguards for civil liberties and enhanced judicial and Congressional oversight.

Mr. Chairman, when I last appeared before the Committee, just 1 month after the President had approved the recommendations of what is commonly known as the WMD Commission, we talked about a recommendation regarding the establishment of an intelligence service within the FBI. I am pleased to report that the FBI's National Security Branch has been established to ensure the integration of the FBI's primary national security programs under the leadership of a single Executive Assistant Director and to implement policies and initiatives designed to enhance the capability of the entire FBI to support its national security mission.

And although still relatively new, the National Security Branch is making significant progress in integrating the missions, the capabilities, and the resources of the Counterterrorism, Counterintelligence Divisions, as well as the Directorate of Intelligence. The FBI is currently working with the Department of Justice and the administration to ensure that the National Security Branch meets the directives set forth by the President and is responsive to the Office of the Director of National Intelligence.

While I am optimistic about the National Security Branch, I am also aware that some harbor doubts about the FBI's ability to transform itself into a leading intelligence agency. Such critics often cite the mistaken believe that the intelligence mission and the law enforcement mission are inherently incompatible. They also contend that the FBI is reluctant to share information with its partner agencies.

I believe it is important to note that both the 9/11 Commission and the WMD Commission found that the intelligence and law enforcement functions should not be separated. They understood that intelligence developed in criminal investigations could be relevant to ongoing intelligence matters. And, in addition, many of the skills necessary to a successful criminal investigation are mirrored in the intelligence arena. The need to cultivate confidential informants

and build rapport with cooperating witnesses, the ability to follow complex money trails, the ability to decipher the coded language of gang members or drug dealers, and the know-how to extract meaning from a collection of seemingly unrelated clues are all skills that can be and are being applied to intelligence matters.

With regard to information sharing, we have doubled the number of intelligence analysts in every field, and in every field office we have established a Field Intelligence Group, or FIGs, as we call them—agents and analysts working together with one shared mission: to leverage intelligence to protect our Nation. From January 2004 through January 2006, intelligence analyst staffing increased on the Field Intelligence Groups by 61 percent, from 617 to 995. This increase in analysts has helped to fuel our sharing of intelligence products. Since September 11th, we have disseminated more than 20,000 intelligence reports, assessments, and bulletins to our partners.

While our National security efforts remain our top priority, we continue to fulfill our crime-fighting responsibilities as well. Public corruption and protecting civil rights are the top criminal priorities for the FBI. Over the last 2 years, our public corruption investigations have led to the conviction of over 1,000 Government employees involved in corrupt activities, to include 177 Federal officials, 158 State officials, 360 local officials, and more than 365 police officers.

Among our civil rights initiatives are our Human Trafficking Task Forces as well as an ongoing review of unsolved or inadequately addressed hate crimes that occurred prior to 1970.

We also continue to focus on violent crime and transnational and national criminal organizations. Operating primarily through our Safe Streets Task Forces and more recently our MS–13 National Gang Task Force, we are working to identify the prolific and violent gangs in the United States. And together with ATF and other Federal and State and local agencies, we are investigating, disrupting, and dismantling these criminal enterprises through prosecution under the appropriate laws.

White-collar crime, particularly corporate fraud, is also an FBI priority. We currently have 15 corporate fraud investigations in which investors in each of these investigations have lost at least a billion dollars. And, in fact, in two of those investigations, they represent $80 billion crimes, and each of those two investigations of those 15. And given the impact of these crimes on corporate America and on investors, we will continue to pursue these cases, as we have done with Enron, Qwest, WorldCom, HealthSouth, just to name a few.

And while I am confident in our intelligence and law enforcement capabilities, our technology must keep pace. As this Committee knows, in March of this year we announced the award of the contract for development of the Sentinel program, and that contract was awarded to Lockheed Martin. Under the terms of the $305 million contract, Lockheed Martin and its industry partners will use proven commercial, off-the-shelf technologies to produce an integrated system that supports processing, storage and management of the FBI's current paper-based record system. The program also includes incremental development and delivery of Sentinel capabili-

ties, including $73 million for operations and maintenance activities.

And now that the contract has been awarded, we are moving forward with phase one of the development process. Each of the four phases will introduce new stand-alone capabilities and will be user-focused. And as each phase is implemented, existing information will be transferred to new systems and older legacy systems will be retired.

I do want to emphasize at the outset that the Sentinel program is not a reincarnation of the Virtual Case File program. Not only will Sentinel provide greater capabilities, it will be deployed on an incremental basis over 4 years. And to prevent any missteps, each phase of the Sentinel contracting process is being closely scrutinized by a team of FBI technical experts, the GAO, the Office of Management and Budget, and the Department of Justice's Chief Information Office, not to mention the Department of Justice's Inspector General. I know that you are to hear from several of these individuals later today. Furthermore, at the urging of Congress, we have also engaged outside experts to help us review and assess the implementation of Sentinel.

And without minimizing the disappointments we have had in the past, I do believe it important to underscore the improvements that have already been achieved in our efforts to modernize the FBI's information technology.

Today, when an FBI agent sits down at her desk and logs on to a computer, he or she is connected at the "secret" level to a fast, secure system that allows her to send e-mails, photographs, and documents to any other agent or analyst in the Bureau—across the country and around the world.

For "top secret" communications, we have deployed the Top Secret/Sensitive Compartmented Information Operation Network, or SCION. And nearly 4,000 personnel have been trained on the SCION network as well as on associated intelligence community systems. The SCION system is the backbone for the FBI personnel to coordinate, collaborate, disseminate, and conduct research on analysis in conjunction with the rest of the intelligence community.

Other technology initiatives, such as the Investigative Data Warehouse, have surpassed our expectations. The IDW is a centralized repository for relevant counterterrorism and investigative data that allows users to query the information using advanced software tools. IDW now contains over 560 million FBI and other agency documents from various previously stovepiped systems. Nearly 12,000 users, including task force members from other Federal, State, and local agencies, can access IDW through the FBI's classified network from any FBI terminal throughout the world.

And we have worked hard to build a solid foundation for the successful implementation of major information technology investments, and these are just a few examples of our successes.

Now, while technology is essential to our mission, it is the men and women of the FBI who remain our most important asset. It is their talent, their creativity, and their commitment to the public good that are the true keys to our success and have been the keys to our success for the 98 years of our existence. Accordingly, we continue to reshape our human resources program to recruit, hire,

train, and retain quality individuals for our expanding human capital needs.

In my prepared testimony, I discuss additional steps we have taken to enhance our human resources, to include the hiring in October of 2005 of a Chief Human Resources Officer with over 20 years' experience in the private sector.

Before I close, Mr. Chairman, I would like to take this opportunity to advise the Committee of a recent report that probably will be discussed by the Inspector General today, but it is a report that highlights the fact that FBI agents are committed to protecting the Nation and are equally committed to the rule of law. As this Committee may recall, shortly after the Republican and Democratic National Conventions in the summer of 2004, media reports stated that the FBI had questioned political demonstrators across the country in advance of the conventions, leading civil liberties groups to allege that the FBI was attempting to chill protesters from exercising their First Amendment rights. At the request of Congress, the DOJ Inspector General conducted an investigation and last week released its final report on the matter. The OIG did not substantiate the allegations and concluded that all interviews conducted by the FBI of potential convention protesters were conducted for legitimate law enforcement purposes and were conducted consistent with Attorney General guidelines.

I am pleased but not at all surprised by the Inspector General's findings. The men and women of the FBI understand and appreciate the power entrusted to them and are vigilant in their efforts to protect the country while respecting civil liberties.

Mr. Chairman, this year will mark the 5-year anniversary of September 11th. The FBI has changed dramatically since the terrorist attacks of that day, and we will continue to evolve to meet the emerging threats to our country. I'd like to invite the members of the Committee to the FBI, either our headquarters or our field offices, to observe this transformation yourselves. You can spend time with the Joint Terrorism Task Forces and the Field Intelligence Groups and see the enhanced technological capabilities available in the field.

I and we are proud of the progress we have made, and I am certainly proud of the dedicated men and women of the FBI who have made our transformation possible.

Thank you for your support of the FBI, Mr. Chairman, and I am happy to answer any questions you might have.

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

Chairman SPECTER. Thank you, Director Mueller.

We will now proceed to the 5-minute rounds of questioning by members.

Director Mueller, on the issue of information sharing, the GAO report in March of this year raises questions about the adequacy of the information sharing. We recollect the hearings which this Committee had back in June of 2002 where we heard from Agent Coleen Rowley and we heard from you about the failure to process the information from the Minneapolis Field Office about Zacarias Moussaoui. And we also had testimony about the difficulties not only within the FBI of understanding the information which you

had, but also on the information sharing. And we now have legislated a new level of bureaucracy with the Director of National Intelligence John Negroponte.

Is the GAO report accurate that there are still problems on information sharing? And to what extent has the new Office of Director of National Intelligence helped, if at all?

Director MUELLER. There is still work to be done in information sharing, but let me point out where we have made substantial strides.

Firstly, the PATRIOT Act has broken down the walls between intelligence and law enforcement exchanges of information. That was a substantial problem before September 11th and was identified as such by the 9/11 Commission, WMD Commission, the joint Congressional inquiry. And so both within the FBI, where we now can initiate investigations—it could be an intelligence investigation that may lead to a criminal violation, or it can be an intelligence investigation that continues on for a period of time. But that wall is down within the FBI. Between the FBI, the CIA, NSA, and other entities in the intelligence community, there is now a free exchange of information.

Most specifically, the National Counterterrorism Center is the hub of intelligence related to counterterrorism. It has access to the information in the data bases of each of the various contributing agencies, and while we collect information according to different protocols—in the case of the FBI, according to the Constitution, the applicable statutes, and the Attorney General's guidelines—nonetheless, that information that is produced is shared at the National Counterterrorism Center where analyses that cut across all of the information are done. That is a tremendous advance in terms of giving us—

Chairman SPECTER. Director Mueller, let me followup with you on that on an informal basis because of the limitation of the 5-minute rounds of questions, and also on an informal basis on the work which the Bureau is doing on technology acquisition and the recent $305 million contract with Lockheed Martin. And let me go to the question of the prosecution of newspapers or newspaper reporters under 18 U.S.C. 798 and 50 U.S.C. 421.

Is it your interpretation of these statutes that Congress intended them to apply to the dissemination of classified information by reporters or by newspapers?

Director MUELLER. Mr. Chairman, I was alerted just before I came in that you may ask this question with regard to the applicability of the statutes. I have not had an opportunity to look at the statutes to determine their applicability. It's been several years since I have looked at them, so I don't feel I'd be in a position to render an opinion on that.

Chairman SPECTER. Well, fair enough. It has come into very sharp focus as a result of a very extensive New York Times article the day before yesterday, so it is true that we have alerted you only recently. I asked that you be alerted yesterday. But if you would take a look, we can talk about that further.

Let me move to the Jack Anderson situation.

Director MUELLER. Yes, sir.

Chairman SPECTER. And the reports that FBI agents have sought the return of materials which Jack Anderson had during his lifetime. If the Bureau wants those back, why not earlier? And why now at all?

Director MUELLER. Well, my understanding—and I'd have to check this—is that we recently came into possession of information indicating that there may be classified national security documents within Mr. Anderson's collection, and the concern was—and our understanding is that collection may well be made available to the public. And so the concern was that there may be documents in there that relate to the national security, may be classified, and the disclosure of those documents may harm the national security.

I think the agents were doing their job in making the inquiry as to whether or not such documents were found or could be found there, and were looking for ways so that we can determine whether or not there are such documents there, and if there are such documents, whether disclosure would adversely affect the national security.

Chairman SPECTER. The red light went on in the middle of your answer, after your answer started, and I am going to observe the time limits meticulously because we have a great many Senators here, and we are going to have a vote at 11 o'clock, so I will come back to that later in the hearing.

Senator Kennedy.

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

The warrantless surveillance issue, 1976, President Ford, Attorney General Levi, welcomed the Judiciary Committee to the Justice Department on four different times; in 1978, we passed the FISA law. Only one member of the U.S. Senate voted in opposition. Collaboration has been successful in the past. We have heard the testimony now from members of the administration that it is not applicable to the current kinds of situations that we are facing on national security.

Now we have a situation where we are putting employees at the National Security Agency at risk. We have criminal and civil cases that are challenging the legality of the administration's program and the warrantless wiretapping. AT&T is back in court. Just this last month the Justice Department has filed its own brief in the AT&T case. Last month three judges on a panel, U.S. Court of Appeals for the Fourth Circuit, sent back a criminal case, saying the evidence obtained during the NSA's warrantless surveillance, questioning whether it was used validly.

How concerned should we be about the current situation where we are seeing the repeated challenges? We have had the American Bar Association say that the actions of the President of the United States have exceeded his authority. We have had the Congressional Research Service say the President exceeded his authority. At other times when this was an issue, we achieved a bipartisan agreement, working together with the administration, that was consistent with the national security and the Nation benefited. Why are we not back into that situation today?

Director MUELLER. I don't believe I can speak to where the Congress is in discussing what if any legislation should be passed to address what you have discussed. I can tell you that I believe there

have been several instances around the country, in cases that are being prosecuted. in which this issue has arisen, but I do not believe any of them has presented an issue.

Senator KENNEDY. Where it has arisen, whether the evidence that has been obtained has been obtained legally, that issue.

Director MUELLER. And my understanding is defense counsel have raised this in several prosecutions, and judges who are—before whom those prosecutions are pending have looked at the issue and determined that the issue is not relevant in those proceedings.

Senator KENNEDY. I think that this is obviously going to continue to be an issue. I think it can be avoided rather simply rather than to have it left out there.

Let me move quickly. In terms of the recruitment by the FBI, in terms of Arab and the Muslim community—I asked you about this in 2003, about the recruitment efforts in Arab-American, Muslim communities. The FBI recruited in the Super Bowl. Can you tell us what the results have been in terms of the recruitment within the Arab and Muslim community in terms of the FBI?

Director MUELLER. Senator, since we last discussed this, we've made substantial efforts to enhance our recruiting. They have been successful, but not as successful as I would like. We continue to encourage members from diverse communities within the United States to join the FBI. I can get you the figures. I don't have the figures off the top of my head.

Senator KENNEDY. OK. Just to followup in this area. Many of us are interested in the challenges on hate crimes. We know anecdotally that these groups, the Muslim and Arab community, have been particularly targeted in the wake of 9/11. The FBI keeps statistics and figures only on anti-Hispanic and other ethnicities, so that it is very difficult from your information that you make generally available to determine how significant this is. Anecdotally, other groups report a rather dramatic increase and spike in this. I would like to be able to sort of work with you to see if there is a way of detecting it. The FBI does provide a range of different kinds of opportunities for local law enforcement in the situations of hate crimes to be able to go ahead and prosecute, and I would like to see if we cannot get a greater focus on it.

Director MUELLER. I do believe we keep statistics. We keep statistics of hate crimes against Muslim-Americans, Sikh-Americans, Arab-Americans, and we can get you those. I can assure you when you look at those statistics, we take every one of these hate crimes investigations exceptionally seriously, and any number of them have been prosecuted at the Federal level as well as the State and local level.

Senator KENNEDY. Just finally—my time is up—on the use of confidential informants, you know well the challenge that we had in Boston, and we have the Inspector General's report, and a situation in New York, and the prosecutions of agents down there. What assurance can you give to the American people that the agents are conforming with the Attorney General guidelines on confidential informants? Now, given the history, we had heard that those are just a few bad apples when we had the Boston situation, a few bad apples in terms of New York, now the district attorney's, up there, vigorous prosecution. What can you tell us that you are going to

do to make sure that we have conformance by the agents with the standards established by the Agency and the Attorney General?

Director MUELLER. Given the circumstance in New York, the protocols relating to our handling of informants changed dramatically. We also have had other occurrences, out on the West Coast, the Leung case. We have—and since that case, we have continued to modify our vetting of our confidential informants, have in place appropriate protocols, do a great deal of education. The training at Quantico hammers on those instances in the past where protocols were not followed.

So we've taken a number of steps to assure that we don't repeat those mistakes of the past. We understand the sensitivity to using sources and informants. And I believe—we put in a series of steps that are being taken to assure the appropriate oversight of those programs, and I believe that the IG's report indicates and acknowledges a number of the steps that we have taken in that regard.

Senator KENNEDY. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Kennedy.

Under the early bird rule, Senator Grassley.

Senator GRASSLEY. Director Mueller, I am going to go through three questions, and I would ask you to take note so I can go through all three, and then you can answer them. They deal with the indictment of the FBI agent in New York, the Inspector General's recent report on the allegations made by Joe Webber about the FBI's lack of coordination with ICE, and last, something about Jack Anderson beyond what the Chairman has already brought up.

In March a grand jury accused former agent Lin DeVecchio of taking bribes and giving secret information to his mafia informant, which led to the murders of four people, similar to the awful Boston scandal a few years ago. Do you think this is going to cause the same sort of damage to the FBI's reputation as those scandals did? Do you approve of the support that this former agent is receiving, because we have current and former FBI personnel publicly raising money for him, giving the impression that the FBI might be circling the wagons to defend the organization and defend one of it own charged with murder?

Second, I did ask you about the Houston terrorism financing case last year. The head of the ICE office said that the FBI was dragging its feet on wiretap application. You agreed that problems at the FBI had caused the delay, and then the Inspector General investigated. So just last week the IG completed his report, but the FBI classified it secret. The FBI should not abuse its classification authority to hide its mistakes from public scrutiny. And I would like to get a commitment from you today that you would work with the Inspector General's Office and me to put together a version of this report that can be released to the public.

And then third, according to Jack Anderson's son, and as closely as yesterday, my staff had an opportunity to discuss with him some of these issues. Some FBI agents recently tried to get the right to take copies of his files by tricking his 79-year-old mother into signing a consent form that she did not understand. They did this by returning to speak to Mrs. Anderson alone after her son, who is also her attorney, made it clear that any permission to take documents would have to be discussed with the entire family. If that

is true, do you think that that is an appropriate investigate technique?

That is the end of my three questions.

Director MUELLER. Let me start with the first one, with the indictment of DeVecchio in New York. That is, quite obviously, not good for him, certainly not good for the FBI. The persons who have shown support for him are either former agents or not agents on duty. Certainly, there was no institutional support when that person is facing such substantial charges in New York.

Second, with regard to the incident down in Houston, or the case down in Houston, we did have a discussion on that. I indicated I would welcome the Inspector General's investigation into that, and my understanding is that portions of it are classified, but there are two point I would make in response to your issue there. And that is, that the report did issue a finding that the FBI did not intentionally delay processing a criminal wiretap application in order to derail an ICE investigation. That was the bottom—that was the finding. I think it's the finding that we discussed when we originally discussed this, that there was a miscommunication and there was delay. And also my understanding is that in a footnote, the IG states the following: the IG found no indications that the FBI over-classified this report to prevent its dissemination.

So my belief is that there is not over-classification. I can tell you from our perspective there is no intent to over-classify the report to prevent its dissemination. That's on the second issue that you raised.

With regard to that, we're very happy to work with you and the IG to find—to try to find a way to produce some summary that is not classified.

Last, with regard to Anderson, I'm not familiar with the circumstances of the interviews there. I do understand at some point there was discussion about perhaps family ties, but I would have to go back and find out more facts about that interview that you advert to, Senator.

Chairman SPECTER. Thank you very much, Senator Grassley.

Senator GRASSLEY. The only thing I would say, if the facts are like I said, that there was an understanding with her lawyer, also her son, that this would be a family matter, then should the FBI go back to a 79-year-old woman and confront her by herself?

Director MUELLER. Senator, I would have to look at the facts of the case.

Chairman SPECTER. Thank you, Senator Grassley.

Senator Leahy, in the capacity as Ranking Member, you are recognized for an opening statement, and beyond that, your turn for a round of questions.

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

Senator LEAHY. Thank you, Mr. Chairman, and thank you for your usual courtesy in such matters. I appreciate you convening today's hearing. I was at a matter with the Commandant of the Marine Corps, and I knew that—

Director MUELLER. Priorities.

Senator LEAHY. —Director Mueller would forgive me for being a little bit late. I think these oversight hearings are extremely important, as I said right after 9/11. In fact, after the oversight hearings that I conducted at that time, we acted in the Congress very quickly to give the Bureau new tools to combat terrorism. We funded information technology. We pushed to correct institutional and management flaws that prevented the FBI field agents from operating at their full potential. I am concerned four and a half years later that the Bureau is not as strong as many of us would like to see.

Director Mueller, you and your leadership team, the hard-working men and women of the FBI deserve, and they have, the constant appreciation of all of us as Americans for the things you do, the sacrifices you make, working tirelessly for decades, especially since 9/11, under great pressure. But the constructive oversight I think is helpful.

You have made great strides in enhancing intelligence gathering capabilities, but I am very disappointed when I find out the FBI has been using those capabilities to conduct domestic surveillance on law-abiding American citizens simply because they oppose the Government's war policy in Iraq. The Seattle Post-Intelligencer reported that Federal Government antiterrorism agencies, including the FBI, conducted surveillance on long-time Quaker peace activist Glen Milner during the 2003 Seafair Festival. A Freedom of Information Act lawsuit has revealed FBI communications about the surveillance of several other domestic peace groups. I think we have all learned Quakers are going to protest wars. It does not make them un-American. It does not make them unpatriotic. In addition Inspector General Fine detailed more than 100 possible surveillance violations reported by the FBI to the Intelligence Oversight Board in the past 2 years.

Senator Grassley talked about Jack Anderson's files. This really bothers me. I did not agree with everything Mr. Anderson wrote. I felt zings from him as everybody else did. But, you know, frankly, there is a concern that the FBI may be going into his files because of some of the things he discovered about J. Edgar Hoover's personal life. I have to tell you, if that turns out—well, don't shake your head—if that turns out to be the reason, for one thing, I cannot see any reason going into his files anyway. I mean it is sort of like all of these things that get classified that have been in the archives for years and years, and suddenly they are classified, or things that are on Government websites, and then when it turns out they screwed up, the documents are suddenly classified. I worry about that.

Last month the GAO issued a report finding that despite more than 4 years of legislation, executive orders and Presidential directives, this administration has yet to comprehensively improve the sharing of counterterrorism information among dozens of Federal agencies, including the FBI. I know you have several initiatives under way to promote better information-sharing, but I look at the terrorist watch list that is produced and disseminated by the FBI's Terrorist Screening Center that has been plagued by too many entries and inaccurate information. We see what happened. I mean Senator Kennedy has just left here, but on one of these terrorist

watch lists, he has had 10 times he could not get on the airplane he has been used to traveling on for 40 years.

I suggested to him that some of these Irish terrorists look alike, but he suggests that may not be it. We had a 1-year-old, less than a year old, whose parents had to get a passport to prove that they were not the terrorists on the list.

We learned that Sentinel is going to cost the American taxpayers $425 million to complete. It may not be done until 2009, and rumor is that the true cost of Sentinel is being hidden by cutting other programs to cover the cost.

So these are concerns that I have. I am concerned that some of the FBI's mid-level and senior-level counterterrorism experts do not have counterterrorism backgrounds. We have given a huge amount of money, and the American taxpayers have given a huge amount of money to the FBI. I worry that it is not being used effectively.

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

I will go ahead and begin my questioning. You can go ahead and set the clock on that.

Chairman SPECTER. We will set the clock at 5 minutes, Senator Leahy, for your round of questioning.

Senator LEAHY. Thank you, Mr. Chairman.

Director, you cited the Inspector General's report and the FBI's investigative activities concerning the potential protestors at both the 2004 Democratic and Republican National Conventions. The report was reassuring as far as it went. But it was limited to allegations arising out of the political conventions, and did not address other incidents where the FBI has been alleged to have improperly targeted Americans based on their exercise of the First Amendment rights. I mentioned the Seafair Festival in Seattle. There is evidence that you have been monitoring other peace groups across the Nation, including the Raging Grannies, scary group if there ever were, a group of elderly peace advocates who sing at events; and the Thomas Merton Center for Peace and Justice, a Catholic peace organization in Pittsburgh. These are groups with no history of violence.

One FBI memo, released pursuant to FOIA request, reads as follows: "The Thomas Merton Center"—that is the Catholic peace organization I mentioned—"is a left-wing organization advocating, among many political causes, pacifism. TMC holds daily leaflet distribution activities in downtown Pittsburgh and is currently focused on its opposition to the potential war with Iraq." This is the memo. The memo is dated a few months before the invasion in Iraq. It goes on to say that TMC's executive director stated to a local reporter that "there are more than a few Muslims and people of Middle Eastern descent among the regulars attending meetings at the Merton Center's East Library Headquarters." And then they say the FBI "photographed TMC leaflet distributors," and "these photographs are being reviewed by IT Pittsburgh specialists." The memo concludes "one female leaflet distributor, who appeared to be of Middle Eastern descent, inquired if the agent was an FBI agent. No other TMC participants appeared to be of Middle Eastern descent."

What possible business does the FBI have spying on law-abiding American citizens simply because they may oppose the war in Iraq? I have said to others, you know, you could save a lot of money and time, turn on C–SPAN. I oppose the war in Iraq, and I say so on the Senate floor all the time. Maybe I should get my FBI report. But go ahead and tell me what possible reasons?

Director MUELLER. Well, Senator, let me start by saying that the IG report—again, there were rumors and there were allegations. The IG report put to bed those rumors and allegations relating to surveillance at the convention. In every instance that we have—

Senator LEAHY. I am not—

Director MUELLER. In every instance we have, Senator—

Senator LEAHY. On Thomas Merton.

Director MUELLER. On that particular case, sir, it was as an outgrowth of an investigation. We were attempting to identify an individual. The agents were not concerned about the political dissent. They were attempting to identify an individual who happened to be, we believed, in attendance at that rally. I'd be happy to have the IG look into that and any other of the assertions or allegations that you made in terms of our investigating persons who are exercising their First Amendment rights.

To my knowledge, we have not surveilled the Quakers. To my knowledge, I have not heard about that group you talk about of the Grannies, and I am very happy to have the IG investigate those assertions, rumors and allegations that may have been spread in the newspapers, to assure that that is not the case.

And I am concerned that raising to this level without a shred of evidence that there is any support for those rumors, that the public have the perception that the FBI is conducting this type of surveillance.

Senator LEAHY. Well, on the Thomas Merton one, the synopsis on the FBI's report is: "To report results of investigation of Pittsburgh anti-war activity." You say not a shred of evidence. Director, this is kind of clear, and if you are talking about—

Director MUELLER. I would be happy to have—

Senator Leahy [continuing]. Anti-war activists, I mean we have a group that meets out in Montpelier once a week. Now, they have been surveilled. Good Lord. There are some people in this country who do not approve of the war. It does not mean they are not patriotic.

Director MUELLER. Well, Senator, if you can give me the facts supporting the proposition that the FBI surveilled that group, I would certainly look into it, and I will ask the IG to look into the—

Senator LEAHY. I am reading it from the Federal Bureau of Investigation's report "to report results of investigation of Pittsburgh anti-war activity."

Director MUELLER. I gave you the background of that report, Senator, and I would be happy to have the IG followup on that.

Senator LEAHY. I am sending somebody down with a copy of it right now. Let us Xerox that and then just give it to him.

Mr. Chairman, my time is up but I will have a number of other questions. I do want to go back to Sentinel, and when I do, Director, I want to ask if other programs in the FBI have been cut back or money taken from them to pay for the Sentinel program.

Chairman SPECTER. Thank you, Senator Leahy.

Senator DeWine.

Senator DEWINE. Thank you, Mr. Chairman.

Director, I would like to discuss the FISA backlog issue. As you will remember, we have discussed this before. In fact, I have been raising this concern with you and with the Attorney General and others for several years. When I asked you about it at a Judiciary Committee oversight hearing in 2004, this was what you said, and I quote, "We still have some concerns and we are addressing it with the Department of Justice, but there is still frustration out there in the field in certain areas, where, because we have had to prioritize, we cannot get to certain requests for FISA as fast as perhaps we might have in the past." End of quote.

Mr. Director, the reason I keep pushing to get this problem fixed is that FISA, of course, is one of the most important tools we have in the fight against terrorism. We need to use it as much as appropriate, and when we use it, it needs to be quick and efficient.

Now, I understand that the use of FISA was up substantially from 2004 to 2005. I have been told that the FISA backlog has now been significantly reduced, but not yet eliminated. This is still a problem in a number of ways and it has a major impact on the FBI because I am told that officers have to have their FISA renewal packages submitted to the FBI 45 days before the FISA warrant expires, because it takes that long for the renewal package to work its way through the FBI, the Department of Justice, and the FISA Court.

I understand that last year there were over 2,000 FISA applications, and that there are currently close to 100 lawyers who work on these issues at the Justice Department. This sounds as though it should be more than sufficient to handle the FISA caseload in a speedy and efficient manner.

Let me ask you a series of questions, and if you could respond to them.

First, why do these backlogs and delays persist?

Second, do you believe we need more attorneys being involved in this? Do you think we need more FISA judges? Do you believe we need changes in the internal review process at the FBI or at the Justice Department?

Further, how does the Bureau of Department of Justice now actually define a backlog? Has there been a change in the definition of what a backlog is? After how many days is a case considered to be part of the backlog? How and when did you arrive at the figure, and are you looking at ways to reduce it even further?

Director MUELLER. Quite a number of questions, Senator, so let me, if I could, address generally the progress that has been made in trying to stay up to date on the FISAs.

We still have to prioritize, although, as you pointed out, the backlog has dropped. The delays are attributable to—can be attributable to a number of factors. It may be the necessity for adding additional facts, in which it goes back to the field for those facts.

But to the bottom line in terms of whether the process would be augmented by additional attorneys, a look at the work flow or additional judges, yes, I do believe that additional resources would assist in terms of attorneys. We continuously are looking at improv-

ing the work flow, particularly with the technology so that documents can be sent back and forth through a dedicated network as opposed to being sent back and forth, which will be a substantial improvement. I do not at this juncture—I am probably not the one to respond to the question as to whether we need additional FISA judges, and I will say that the additional FISA judges that we did—well, the FISA Court as a whole is working exceptionally hard, as you can tell from the number of applications that they reviewed. I, as well as anybody who reviews these applications, would welcome some mechanism to reduce the amount of paperwork that goes in each application. Each application is approximately a half inch thick in terms of paper, and compiling all that paper and putting it in a package for the Court is a substantial process. All of us would benefit from having a procedure that was somewhat expedited.

My expectation is that with the establishment of the National Security Division at the Department of Justice, that in addition to the deputy's office, which is looking at this, we will have another actor over there that is looking at these issues.

Senator DEWINE. Definition of backlog is the same definition? Are we comparing apples to apples?

Director MUELLER. I would have to go and look at the definition, but I have no reason to believe that we're not comparing apples to applies. Certainly, nobody is trying to change the—I have not seen—and I get a breakdown every month—I have not seen a change in the reporting in any event, much less to make it appear that the backlog was reduced.

Senator DEWINE. Well, my time is up, but the summary would be more attorneys would be helpful; somebody else can make the decision about judges; reduced paperwork would be helpful; expedited process would be helpful.

Director MUELLER. Yes.

Senator DEWINE. Thank you.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator DeWine.

Senator Feinstein.

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

Welcome, Mr. Mueller. I wanted to ask you three questions. I will try to be brief, and if your answers could as well, I can get through the questions.

In 5 years you have had six different heads of Counterterrorism, and six different executive assistant directors overseeing Counterterrorism. Last week, Gary Bald, the new head of the National Security Branch, announced that he too is leaving. What is the reason for this high turnover? What are you doing about it? And do you ask people when they join that they be required at least to stay for a period of time?

Director MUELLER. Putting it in perspective, there are a number of factors that have contributed to the turnover. The first is, you take somebody like Gary Bald, who I'll use as an example. He has 30 years of service to the FBI and to the country. He has kids in college. He has worked in counterterrorism for at least the last four or 5 years, whether the head of the Counterterrorism Division, and then head of the National Security Branch. He had a tremendous

opportunity for both him and his family that would be very difficult for him to continue. So the opportunities outside, particularly since September 11th, where everyone wants a security director, and the obvious fact that many of these corporations can pay far more than the Federal Government is a factor. The fact that a person has spent 30 years in the FBI in a career and still can have a second career, and has to make an earlier decision, is a factor. And the last factor is that we work 24 hours a day, 7 days a week, and it's a lot of pressure on persons in those positions.

Senator FEINSTEIN. Let me stop you for a moment. How long had he been in the job?

Director MUELLER. How long had he been in the job? As the head of National Security Branch, probably 6 months.

Senator FEINSTEIN. Doesn't he consider that before he takes that job?

Director MUELLER. He does—

Senator FEINSTEIN. I mean these are critical jobs at a critical time, and it would seem to me that somebody would not take a job for 6 months and then accept something else that came along. It would also seem to me that in terms of management practices, this ought to be advised against, counseled against, and if somebody cannot give you a commitment of time, why hire him?

Director MUELLER. I understand what you're saying, and it is an issue we're wrestling with. I will tell you that since September 11th we have developed, I think, a very strong bench, particularly in counterterrorism. We have a number of people who have been working in counterterrorism before September 11th who are coming along, and a strong bench of those who have worked in counterterrorism solely on that issue since September 11th.

Senator FEINSTEIN. All I am saying is you have had six different heads, and I think that is a problem.

Director MUELLER. I understand that.

Senator FEINSTEIN. Now, today the Washington Post indicates that you have filed 9,200 national security letters and 2,072 FISA Court warrants. I was interested in Senator DeWine's questions. I have written a letter to the Attorney General asking him process questions, and he has not responded. We have asked a second time. He still has not responded. I am a member of that Subcommittee looking at the National Security Administration's electronic surveillance program. How much time does the FBI need to get a FISA warrant? What is the average time? You have clearly gotten 2,072 of them, if the press is correct. What is the average time it takes to process a FISA warrant?

Director MUELLER. I would have to provide you those figures, and it would require going back and looking through records to provide you those figures, and the difference would be between an emergency FISA application and a non-emergency FISA application, quite obviously.

Senator FEINSTEIN. Can you also tell us how many of these 2,072 were emergency?

Director MUELLER. I cannot off the top of my head. I can provide you those figures.

Senator FEINSTEIN. If you would, I certainly appreciate that.

Director MUELLER. Yes.

Senator FEINSTEIN. Let me ask the third question then. In his written statement, Inspector General Fine notes that there is shared responsibility for port security between the FBI and the Coast Guard, but that confusion exists over each agency's authority, affecting the ability to establish a clear and effective command structure. General Fine states that the response to a maritime incident could be "confused and potentially disastrous." That is a quote from the report.

These are strong words, and this is clearly unacceptable. What is the FBI doing to address this concern and the other 18 recommendations of the IG?

Director MUELLER. We're addressing each of the recommendations of the IG, I can assure you. And with regard to the responsibilities, there is a preliminary agreement that we had with the Coast Guard in terms of our responsibilities being in the investigation arena, as opposed to the interdiction arena that generally would be the Coast Guard. Now, we are working with DHS and the Coast Guard and discussing how we can be more precise in the allocation of responsibilities.

Senator FEINSTEIN. I might say that if I were the Director and saw this response from a very good IG, and his comment is the response to a maritime incident could be "confused and potentially disastrous," those are very strong words.

Director MUELLER. They are strong words. I will tell you that we've had a number of incidents—

Senator FEINSTEIN. It seems to me it ought to be beyond "I am going to look into the situation."

Director MUELLER. Well, we have had a number of incidents over the years in which we have worked very closely with the Coast Guard. I have every confidence—I understand the words that Mr. Fine used. I understand they're strong, and I understand his concern. And we are addressing that concern in terms of developing a new MOU as opposed to the draft MOU that we have been working on for a number of years. But I'm also comfortable and confident, based on our working with the Coast Guard in the past on any number of incidents, that depending on the incident, the appropriate personnel will be brought to bear. And so I don't want the impression left that I'm not concerned about it. I am concerned about the IG's finding. I am concerned that we reach a more formalized understanding quickly, but I am also comfortable and confident that our relationships with the Coast Guard and the way we handle these incidents together, based on our history, would indicate that such an incident, as it came along, we would allocate the appropriate responsibilities and move forward.

Now, I understand what Mr. Fine has said, and we are moving to address that.

Senator FEINSTEIN. Thank you. I am over my time.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Feinstein.

Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman.

Welcome, Director Mueller. I have two questions for you. The first had to do with the Brandon Mayfield case. And as you know, Mr. Mayfield was a lawyer in Portland, Oregon, who was arrested

for allegedly, or was under suspicion of participating in the Madrid bombing. First of all, I want to tell you, as someone who supported the PATRIOT Act and its reauthorization, I am glad to see that the Inspector General found that the Government did not misuse any provisions of the Act, but I am troubled by some of the reported actions of the FBI in this case.

Some of the missteps found by the Inspector General were that the material affidavit and report of the arrest of Mayfield contained several inaccuracies, including an "unfounded inference" regarding fake travel documents. The FBI Lab's arrogance caused it to disregard questions raised by other professionals, and once the mistake was made public, the FBI made several statements as to the cause of the misidentification, which turned out not to be true.

I know the Office of Professional Responsibility is in charge of the investigation, and I do not know where the investigation stands, but I certainly hope that strong actions will be taken if these are indeed the facts, to make sure that these sorts of things do not happen in the future.

Would you like to comment on that?

Director MUELLER. Yes. The report is absolutely accurate in terms of we made a mistake, that our examiners—I'm not certain I'd use the exact same word, "arrogance," but certainly self-assurance, where they shouldn't have been self assured, particularly when the authorities in Madrid had questioned it. There should have been a reevaluation of it, a much closer review of it than was done at that time. It was unique in that there was significant similarities between the prints, but that's no excuse. We should have done a better job. We made a mistake on those prints.

And I can tell you we have taken steps. Where the IG has indicated actions need be taken, we have taken each of those actions. Indeed, before the IG report, we had brought in a panel of experts ourselves to look at our processes to assure that to the extent that we could change those protocols to make certain that this didn't happen again, we did. So we want to make certain it does not happen again.

Senator CORNYN. With regard to the IG's statement that the FBI made several statements as to the cause of the misidentification that were not true, can you tell us any more about that?

Director MUELLER. I'd have to go back and look at the specifics of that. That did not hit me as the most important aspect of what the IG told us in that report.

Senator CORNYN. I want to followup on a question Senator Kennedy asked you about noncompliance with the Attorney General's guidelines with regard to the use of confidential informants. He mentioned that. But I was struck to see that the report of the Inspector General found that there were one on more guidelines violations in 87 percent of the confidential informant files that were examined, including 49 percent noncompliance with FBI agents giving proper instructions to informants.

As you know, there are serious and high-profile problems that were mentioned in Boston, there were some in Forth Worth, with regard to the misuse of informants, and also in a another law enforcement agency, ICE. I have been seeking information about an ICE informant, who has been involved in multiple murders while

under ICE's control. Can you tell us what you are doing at the FBI to improve compliance with the Attorney General's guidelines?

Director MUELLER. Yes. In the wake of the IG's report, we have gone out—an education program, an assurance from top-down that documentation, appropriate documentation is done in the files to assure that the files reflect the work that has been done by the Agency in handling the informants. I believe the Inspector General is familiar with the change of protocols in the wake of the Leung case out in Los Angeles, so it is a combination of changing the protocols, training of agents so they better understand what is required in terms of handling informants, and last, assuring that particularly in our inspections and the like, we make certain that we cover those issues.

Senator CORNYN. Thank you very much.

Chairman SPECTER. Thank you very much, Senator Cornyn.

Senator Feingold.

Senator FEINGOLD. Thank you, Mr. Chairman.

Director Mueller, as you reference in your testimony, the PATRIOT Act Conference Report requires the Inspector General of the Justice Department to complete a comprehensive audit of the FBI's use of national security letters and Section 215 business record orders. And I understand that that audit is under way. Is that right?

Director MUELLER. I believe that is correct. And I will turn to Mr. Fine, yes.

Senator FEINGOLD. I note that the Inspector General indicated that it is.

In the President's signing statement, he suggested that he may not share the results of this audit with Congress, in direct violation of the Conference Report requirements. Will you commit to me today that you will fight within the administration to allow these audits to be shared with Congress, in a classified setting, if necessary, so that we can fulfill our oversight responsibilities?

Director MUELLER. Needless to say, I'm bound by the administration, but I see no reason why the report could not be shared in some context with Congress.

Senator FEINGOLD. So you would fight for that, given the clarity of the law.

Director MUELLER. All I can say, that I can see no reason why it would not be shared with Congress. I note that that Congress has been—there was a report that came from the Attorney General on the number of national security letters that have been issued in the last year. So my expectation is that they'll be disclosed to Congress. I see no reason why they should not.

Now, whether I go out there and fight for it is another issue. I will tell you that I see no objection to providing it to Congress.

Senator FEINGOLD. I have a lot of regard for you, and I think you should fight for it. I mean, this is the law, and I would hope you would commit to fighting within the administration to comply with the law in this case by making this information available. But, I do not take your answer as being a refusal in that regard, and I look forward to your active role, if it becomes necessary.

Director MUELLER. Yes, sir.

Senator FEINGOLD. Unfortunately, the President's signing statement on the PATRIOT Act is hardly the first time that he has

shown a disrespect for the rule of law. The Boston Globe reported on Sunday that the President has used signing statements to reserve the right to break the law more than 750 times, and as we all know too well, he secretly authorized Government officials to violate the FISA law for more than four years, and continues to do so.

Mr. Director, the President's action raised some difficult questions for those of us in Congress. Take the PATRIOT Act. We completed our work on reauthorizing the PATRIOT Act in March. How can we know whether the Government will comply with the new laws that we passed? I am not placing the blame on you, obviously, or your agents, who work to protect this country every day, but how can we have any assurance that you or your agents have not received a secret directive from above requiring you to violate laws that we all think apply today?

Director MUELLER. Senator, I am not familiar with the particular signing statements that you discuss, but I can assure you with regard to the FBI, that our actions will be taken according to appropriate legal authorities.

Senator FEINGOLD. I appreciate that, and all I can say is that if somebody had told me back in November when we were debating the PATRIOT Act that I would feel it necessary to ask the FBI Director for assurances that he and his agents were not being directed by the President or the Justice Department to violate the PATRIOT Act as Congress wrote it, I would not have believed it, and yet, here we are. But I appreciate, obviously, your answer.

Mr. Director, on Friday afternoon, the Justice Department released information about the use of national security letters and orders under Section 215 of the PATRIOT Act, and that report states that in 2005, the Government made, and the FISA Court approved, 155 applications for Section 215 orders to obtain business records and other tangible things. The report also states that in 2005, 9,254 national security letters were issued related to U.S. citizens or lawful permanent residents. I would like to just ask a few quick questions about those statistics.

First of all, the report does not cover NSLs concerning individuals who are not U.S. persons; is that correct?

Director MUELLER. I'm not certain on that.

Senator FEINGOLD. It seems to me that your staff agrees.

Director MUELLER. My staff indicates that you're correct.

Senator FEINGOLD. Thank you, Mr. Director. And it does not include NSLs issued to obtain phone and Internet subscriber information; is that not correct?

Director MUELLER. That is also correct.

Senator FEINGOLD. So the report does not cover the sum total of all NSLs, obviously.

Director MUELLER. Correct.

Senator FEINGOLD. But despite those facts, the number of NSLs in this report is far, far larger than the number of Section 215 orders. Why is there such a disparity between the use of Section 215 orders and the use of national security letters?

Director MUELLER. I'd have to get back to you on that. I haven't given that much thought. Senator, I have to get back to you with an answer on that.

Senator FEINGOLD. I look forward to that, because I fear that the reason might be that under Section 215 they have to go before a judge, and they do not with NSLs.

Director MUELLER. That is true.

Senator FEINGOLD. And if that is not the reason, I look forward to whatever light you can shed on this in the future.

Director MUELLER. That's true, you do use—the number of NSLs that you mentioned was in excess of 9,000, but it is on 3,500 persons. In other words, one person could have had a number of NSLs, seeking different pieces of information on that particular person.

Senator FEINGOLD. I understand that, but it is still a great disparity, and it may point to the need for even greater protections with regard to the NSLs.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Feingold.

Senator Sessions.

Senator SESSIONS. Director Mueller, I appreciate your service and the long professional history and background you bring to the position that you hold.

When Director Ridge left, not long after he left, he said, if I had one bit of advice to give to my successor at DHS, Department of Homeland Security, it would be that we have a biometric identifier for those who come in and out of the country, and it be the fingerprint.

You and I have talked about that before. Based on your experience in law enforcement, the base use of fingerprints throughout our system, would you agree that as we move forward to create a more workable entry-exit system into our country that we do need a biometric identifier, and the fingerprint would be the best idea there?

Director MUELLER. I believe that the fingerprint should be the foundation biometric, but I know a number of people, including at DHS, are exploring the addition of other biometrics that would even give you more certitude in terms of individuals, but, absolutely, the fingerprint should be the foundation biometric that we use.

Senator SESSIONS. That is good. I think it should be the basis because if you come up with a new system, the people that have been arrested in the United States for crimes that have had their fingerprints made a part of the record, they would not be picked up by a new system, would they?

Director MUELLER. That's correct, they would not. But additionally, as you, a former prosecutor, know as well as I do, that fingerprints are left at scenes of crime. It can be in a cave in Afghanistan. They can be left in a safe house in Iraq. And when those latent prints are fed into the fingerprint system, matches are possible that you would not have with any other biometric system, which is an additional reason why, in my mind, the fingerprint should be the foundational biometric.

Senator SESSIONS. And FBI manages the fingerprint system nationwide.

Director MUELLER. We do, yes.

Senator SESSIONS. There is no capacity problem that you know of that could not be solved that deals with the additional fingerprints that might need to go in the system?

Director MUELLER. No. We have on the drawing boards and are seeking money from Congress for the next iteration of that fingerprint system.

Senator SESSIONS. The Inspector General completed a sixth review that examines efforts to integrate the Federal law enforcement and immigration agencies' automatic fingerprint data bases. It has not been done yet, and we have been working on that for quite some time, to allow law enforcement and immigration officers to more easily identify criminals, known or suspected terrorists entering the United States. The review is continuing to assess the FBI and DOJ actions since December of 2004 to achieve full interoperability of FBI and DHS, Department of Homeland Security, fingerprint systems. Do you think that is important? How far away are we from making that happen?

Director MUELLER. It is important. The Inspector General has looked at this over a number of years. I give a lot of credit to Mike Chertoff for understanding that we needed to be on the same page, and I think since 2004 we've made substantial strides in resolving that issue.

Senator SESSIONS. Let me tell you what I think the problem is. The American people are being asked to accept a new and generous immigration system. They are also being told that we are going to create a system of entry and exist, both at our airports, our ports and our borders, that will actually work. It seems to me that the American people have a right to be concerned that on matters like this that has taken so long, the entry-exit systems that still are not in place yet, many of which are not part of your bailiwick, not part of your responsibility, but I think we have a right to ask and expect that by the time we create any new immigration system, that this would be a big part of it.

First I will ask you, don't you think an effective entry-exit system is important, and I understand you to say that fingerprints are a key part of that?

Director MUELLER. Yes. Yes, to both.

Senator SESSIONS. Thank you, Mr. Chairman.

Chairman SPECTER. Thank you very much, Senator Sessions.

Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman. Thank you, Director Mueller, and I thank you for your efforts to help bring the FBI into the 21st century. It is a big job.

The first question I have is on surveillance programs. In March, the U.S. News and World Report published an article in which they claimed that the same legal reasoning that the administration used in defense of secret NSA electronic surveillance was floated as support for warrantless physical searches. According to the article, you were alarmed and personally very concerned, not only because of the blow-back issue but also because of the legal and constitutional questions raised by warrantless physical searches. Is this true?

Director MUELLER. I am not familiar with any discussions about utilizing an authority, whatever authority, to undertake warrantless physical searches?

Senator SCHUMER. So was U.S. News wrong in that?

Director MUELLER. I do not know what the reporter at U.S. News is talking about.

Senator SCHUMER. OK. So let me ask you the question: Would you have legal or constitutional concerns about the use of warrantless physical searches in the United States?

Director MUELLER. Yes.

Senator SCHUMER. That is a quick, straight, and to-the-point answer.

To your knowledge, has the FBI conducted any such searches?

Director MUELLER. No.

Senator SCHUMER. Is it possible that such searches could have been conducted by FBI agents during your tenure without your knowledge?

Director MUELLER. It's possible, but I would doubt it.

Senator SCHUMER. OK. The article also mentions that both you and Jim Comey had concerns about the NSA domestic surveillance program that the President has confirmed because you were worried about the ability to use any evidence that it might have gathered in court. Is this true?

Director MUELLER. I really believe I shouldn't go into discussions I may have had with others in the administration.

Senator SCHUMER. OK.

Director MUELLER. And to the extent that there were concerns, there was an OLC opinion that supported the legality of the NSA program.

Senator SCHUMER. But you—well, let me ask you: Do you have concerns? Do you believe evidence collected by the NSA without a warrant could be successfully challenged in a criminal prosecution in court?

Director MUELLER. I would say that there have been a number of cases so far in which this issue has been raised, and my understanding that in each case the judge who is presiding over the trial has not found it to be an issue.

Senator SCHUMER. OK. Let me ask you this: Is there anything wrong with the Committee seeing the OLC opinion?

Director MUELLER. That's out of my bailiwick. That's up to the Department of Justice.

Senator SCHUMER. Well, what do you think? Why shouldn't—I mean, there is so much secrecy about this whole thing, and I think it drives people on both sides of the aisle—well, it makes us upset.

Director MUELLER. I think that's an issue to be taken up with the Department of Justice. I have no say over what is released from—particularly when it's not our document.

Senator SCHUMER. OK. Next I would like to ask about watchlists. We all know what watchlists are. They are important. But according to one report, there were several watchlists at one time, terrorist watchlists.

Director MUELLER. True.

Senator SCHUMER. And the President set up a Terrorist Screening Center to consolidate and streamline this information, making sure it is accurate and effective. That is a common-sense idea.

It is now 5 years, and we still do not have an accurate, comprehensive data base, according to the Inspector General Fine's tes-

timony. And what is more, the Inspector General's office anticipates it will take several more years for the Terrorist Screening Center to fully review the records for accuracy and completeness.

First, do you agree with that assessment?

Director MUELLER. Yes, sir. Records, when you combine the records from no less than, I think, 12 separate agencies in order to obtain a comprehensive terrorist list where there have been any number of agencies that have contributed the information that has put a name on a terrorist list, yes, sir, there are inaccuracies. I know that the Terrorist Screening Center is working hard, very hard. They have prioritized to eliminate those inaccuracies, but because of the size of the list, yes, it will take some time.

Senator SCHUMER. Do you think 5 years?

Director MUELLER. I can't—

Senator SCHUMER. You know, it is taking so—I mean, we understand that these things take a while, but whether it is computers or these watch lists, I mean, it seems to me that just from my small knowledge of this and of corporate America, if a corporation, a large corporation—an IBM, a General Electric—had this problem, it wouldn't take them 5 or 7 years to solve.

Director MUELLER. Well, they may have the personnel and the moneys to put to it. But I can tell you that we—

Senator SCHUMER. Do you not have enough—

Mr. MUELLER [continuing]. Have over 200,000 names that have to be vetted. That takes a long time.

Senator SCHUMER. Do you have adequate—if we gave you more personnel and money, could you do it quicker?

Director MUELLER. Yes.

Senator SCHUMER. OK. Just one final question. The OIG made 40 recommendations for improving the TSC. Do you intend to follow all of them? What steps have been taken to follow these recommendations so far? How many remain largely undone?

Director MUELLER. I'd have to get back to you. In general, almost—I think Glenn Fine would tell you almost to a one we follow the recommendations. Occasionally, there are one or two that we disagree on and we'll have a discussion.

Senator SCHUMER. I would ask, Mr. Chairman, unanimous consent that the Director be given some chance to answer that in writing with a little more specificity. I don't expect it here.

Chairman SPECTER. It is acceptable to have him submit written responses. Thank you very much, Senator Schumer.

Senator SCHUMER. Thank you.

Chairman SPECTER. Senator Durbin?

Senator Schumer. You are willing to submit those, I take it?

Director MUELLER. Yes, sir.

Senator SCHUMER. OK, thanks.

Chairman SPECTER. Senator Durbin?

Senator DURBIN. Thank you, Mr. Chairman. The microphone is still warm.

When we reauthorized the PATRIOT Act, one of the major concerns was its impact on libraries. And we felt, when we wrote the language—I use that term loosely because I did not specifically write that language, but Congress—that we had finally cleared it up, that unless a library was an Internet provider in its traditional

function of just providing Internet services to its customers, that it would not be subject to an NSL. Is that your understanding now under the reauthorized PATRIOT Act?

Director MUELLER. I'd have to go back and look at the specific language. I can tell you that we have not—well, you've made the distinction between a library serving as an Internet service provider, which is one sticking point. I'd have to go back and look at the specific language, or could you hold just 1 second? Let me see if I could...

[Pause.]

Director MUELLER. We would have to go back. It's somewhat of a complicated provision. I'd want to be precise in my answer to you. So I'd appreciate the opportunity to go back and take a closer look at it.

Senator DURBIN. We felt that we had finally put to rest the concerns of the library community that there were only a handful of libraries across America that served as Internet providers that may have been subject to the NSLs under the new reauthorized PATRIOT Act. And so if you would be kind enough to come back with, as explicit as you can, your understanding as to whether we accomplished in your eyes what we set out to do.

Director MUELLER. OK. I will say—there is one item you said that I'd probably take exception to, and that is, there is but a handful that are Internet service providers, and maybe the distinction between an Internet service provider and one who provides computer services in a library, because many, many libraries now across the country provide computer services.

Senator DURBIN. I will tell you, on the basis of what you just said we are going to be inundated by libraries now who thought this was cleared up. Please look at this—

Director MUELLER. I did not mean—I will give you a precise answer. I did not mean to confuse the issue at all.

Senator DURBIN. Please give us a timely answer, because there is a genuine concern across America in this community, and we felt we had finally put it to rest. And I wanted to hear those words from you so that I could sleep easy. But now I am going to have restless nights until you get back. Please do that as soon as you can.

Let me move to another issue. A great source of frustration that we run into is when people are going through the naturalization process and they have to be subject to basic fingerprint analysis by the FBI. And the timing of this analysis is now a matter of grave concern because it is taking longer and longer for the FBI to complete this fingerprint and background check.

Could you tell me if you are monitoring this, particularly in light of our current debate, which could dramatically expand the number of applicants for naturalization?

Director MUELLER. Yes, I will have to get back to you on that. I did not understand that to be the case, but I will check on that and get back to you.

Senator DURBIN. A serious issue. When we contact Citizenship and Immigration Services, they point the finger at you. They usually claim the background check is pending at the FBI. Now,

maybe that is a convenient excuse. Whatever. I am sorry. I said "fingerprint check." I meant "name check."

Director MUELLER. Oh, name checks.

Senator DURBIN. Name check, please, if you could address that.

Director MUELLER. Yes, that has been on my radar screen, and we have been addressing that, and there is a very small percentage of name checks that we do not get back to very quickly. But I will have to get you those statistics.

Senator DURBIN. OK.

Director MUELLER. I know that that has been a concern.

Senator DURBIN. Thank you. I apologize for confusing that.

You and I have had a long conversation about technology, and I am certainly not an expert at that nor claim to be. But it appears that you have been through several major crises with that, starting with what you inherited at the FBI. I guess the kindest thing to say is one failed attempt to try to reform the system at great expense, and now you are involved in another attempt. Can you just tell me how I would explain to people why this became so complicated with the FBI to establish a modern computer system?

Director MUELLER. I would reframe the question a wee bit in the sense that, yes, we had problems prior to September 11th. We have had any number of technological successes since then, all of which are overshadowed by the failure of one aspect of the Trilogy project. That is the Virtual Case File. People do not acknowledge that we have put new computers on everybody's desk. So we put through the—put down the local area networks, the wide area networks. We have IDW, Investigative Data Warehouse, all of which we have brought on board since September 11th.

When it came to Virtual Case File, I had to make the decision that I could not spend another $50 million in a system that they could not assure me was going to work and it was time to bite the bullet. The contract we have with Lockheed Martin now is a phased project over a period of time. We have learned our lessons. We have built up our CIO shop. We have an enterprise architecture. We have a contractor in which I have a great deal of faith. We have done a much better job in setting out our requirements beforehand.

I will be meeting with the CEO of Lockheed Martin every quarter, and I believe that we have turned the corner and are on the right track, and I believe—and I'd paraphrase something that the IG said. I think he said in one of his reports, scrutinizing this, that we appear to be on the right track now. I believe we are on the right track.

Senator DURBIN. Thank you, Mr. Director. Thank you for your service, and I am going to give you for your staff to review a colloquy between Senator Sununu and myself on the library issue and NSLs, which I hope you will look at in a timely fashion and respond to as quickly as you can.

Thank you, Mr. Chairman.

Chairman SPECTER. Thank you, Senator Durbin.

Director Mueller, we are near the ending of a vote. Senator Leahy and I are going to go vote, and we will be right back.

Director MUELLER. Yes, sir.

Chairman SPECTER. Thank you.

Senator LEAHY. Mr. Chairman, I will also give him a copy of this. I told you I would give you a copy of the investigation in Pittsburgh. I have it. I will bring it down.

[Recess at 11:08 a.m. to 11:29 a.m.]

Chairman SPECTER. Director Mueller, in asking you the question about the FBI action to retrieve papers from Jack Anderson's estate, it is part of an overall concern about the increase of executive power where a great many things are happening, and this Committee has not been able to get answers to a great many questions. And you are the ranking officer of the principal investigative agency of the executive branch and have very widespread law enforcement authority, both as to crimes of violence and terrorism and intelligence gathering. And I have some specific questions in a context of a concern which this Committee has about the expansion of Executive power.

We have seen a pattern of activity. We have seen the incarceration of a reporter in a context where a grand jury has convened because of the disclosure of the identity of a CIA agent—a very serious national security matter. The focus of that grand jury shifted away from that to a question of perjury, which is also serious, but not at the level of national security. This Committee has had hearings and is preparing legislation introduced by Senator Lugar, and the legislation which we are preparing draws a sharp contrast between a reporter's answering questions that relate to national security as opposed to perjury.

And it seems to me that a case may be made—I am not saying it should be, but may be made for a contempt citation for national security, but not for perjury. Perjury is important, but these are all relative matters.

Then you have the introduction of the President's signing statement and what impact that may have on the interpretation of laws. You and I worked very hard to get the PATRIOT Act finished, and I appreciated your comment on what we have done in a balanced bill.

We are going to have a hearing on that later, but what is a Presidential signing statement? You will be happy to know I am not going to ask you that question. I have got too many other questions for you. We are going to reserve that until later. And I say this with great respect to President Bush. This is an institutional issue, and he and I have had many conversations about the difference between the President and the Presidency. And the issue which we have on this surveillance program is an institutional issue.

And there is the eight-page Attorney General's letter of October 15, 2002. I cannot remember seeing such a complicated exposition on a statement by the Attorney General, which starts off, "The President and I place deterring, detecting, and punishing unauthorized disclosures of U.S. national security secrets among our highest priorities." And then he goes on and on and on as to how they are going to deal with it.

He sends this letter to Speaker Hastert. Then he sends a copy to Vice President Cheney. I am not going to ask you why he sent a copy to Vice President Cheney either. Maybe it is because Speaker Hastert is the presiding officer of the House and the Vice President is the presiding officer of the Senate.

Now the NSA program, the electronic surveillance, there is an investigation into a leak, and there is a suggestion that not only the reporter but the newspapers—or perhaps more importantly, the newspapers and the reporter are subject to prosecution.

Now, that is in a context where the executive branch is violating the National Security Act, which requires disclosing information to the Intelligence Committees—not the Gang of 8, although as a matter of custom, that has been going on in Democrat and Republican administrations for a long time, and as Chairman of the Intelligence Committee in the 104th Congress, I was a member of the Gang of 8. And I can tell you we didn't find out very much. The Vice Chairman of the Senate Intelligence Committee, a member of the Gang of 8, has a handwritten letter, which has been published, to the Vice President complaining that he could not understand the program, that he did not have access to a lawyer to discuss the program, that he did not have an assistant to help him with the program.

And let me come to a couple of questions in this context where you have the electronic surveillance program disclosed by the New York Times. It was disclosed on December 16th, right in the middle of our final day of argument on the PATRIOT Act. We had a hard time getting the PATRIOT Act passed. I think we might have gotten it passed if that disclosure had not been made on that day. Senators on the floor said they were in doubt or perhaps inclined to support the Act, and when they read about that story, they were against it. But to manage a bill like the PATRIOT Act, with all the complications, and to have that explode in my face was a real problem in trying to get some legislation through. And I committed to hearings, and we have had four hearings. We have not found out very much because the Attorney General will not tell us anything. And Senator Leahy, ardently, and others want to bring him back, and I am not going to bring him back in a futile effort.

So here you have the NSA Program which, on its face, violates the Foreign Intelligence Surveillance Act. I do not give any credence to the argument that it was authorized by the resolution for the use of force. But if the President is using Article II powers, that trumps the statute. And I raised this issue with the President last week. He called a group of us in to talk about Sherman and talk about his agenda. And he said, "Are you saying I am doing something wrong?" And I said, "No, I am not saying that, Mr. President. I don't know whether you are or not because I don't know what the program is." And if you're dealing with Article II powers, you have to have a balance. The Supreme Court has made it plain and no one disputes the fact that the President doesn't have a blank check. So it is a question of what is going on.

Let me ask you specifically about your investigations as to reporters and as to national security cases. Do you agree with me that there is a sharp distinction between holding a reporter in contempt where there is a national security issue involved, like the disclosure of the identity of a CIA agent, as opposed to a perjury issue before a grand jury?

Director MUELLER. Senator, I think it would be a question of the context, although certainly being charged and convicted of a crime

is different than being held in contempt. In other words, in terms of the penalty, quite obviously it is different.

Now, you are also talking about the difference between a perjury investigation and a disclosure of national security investigation. And I think it depends on the circumstances. I would note that in the case to which you are adverting, there was a judge who had to make the determination as to whether contempt was appropriate. In other words, it was not solely the executive's decision to make, but to hold the reporter in contempt, there had to be a showing and a judge had to make a determination as to the necessity for the information, and I presume made the determination taking into account the seriousness of the crime.

That is about all I can—

Chairman SPECTER. Well, you have not answered the question, Director Mueller.

Director MUELLER. There is certainly a difference between perjury and between—

Chairman SPECTER. Well, you have cited differences, but the question is: Should Congress deal differently with a shield law for reporters on a national security issue like the disclosure of the identity of a CIA agent contrasted with a perjury investigation?

Director MUELLER. Well, I can say generally, without knowing the context, certainly a national security violation may be far more—have a far more adverse impact on the public than a perjury violation. But talking generally, yes.

Chairman SPECTER. Well, that is some help, although my view was pretty well established before your answer. I want you to take a look at these statutes on unauthorized disclosure, and when the New York Times writes about the considerations by the administration about criminal prosecutions under these statutes for newspapers and reporters, that is something which is a matter of the jurisdiction of this Committee as to what those statutes mean. The courts have to interpret them, but they interpret Congressional intent. And there is a very learned article by two professors from Columbia, Harold Edgar and Ben O. Schmidt, where they raise questions about these statutes, and come to these conclusions: "There has to be a balance of the information, defense significance against its important for public understanding and debate." And they say that in the absence of a showing of Congressional intent to go after newspapers, that "to whatever policy may become compromised by newspapers' disclosure or defense information, there has to be a balancing." Given the absence of Congressional intent, "doubts about whether to protect the efficacy of disclosure rather than stress its adverse security consequences should be resolved on the side of public debate." They raised a question about whether "selective enforcement is a real danger."

But the newspapers have traditionally done a very important job in our society on exposing governmental wrongdoing, Senators' wrongdoing, corruption in Government. This Committee gets a lot of its leads on what we read about in the paper. There is a lot more oversight provided by the press than there is by the Judiciary Committee. It may even be that the FBI gets information leads as to what you do from what—may the record show an affirmative nod. We are making a little progress, just a little, Director Mueller.

Let me say for the record that I have a very high regard for Director Mueller, and we have had a longstanding relationship, and I have a very high regard for the FBI. And as an Assistant DA, I used their evidence to convict the Philadelphia Teamsters. On the Warren Commission, we used their investigative resources to develop the single-bullet theory—not giving you the blame for it, not giving your agency the blame for it, Director Mueller. But I would like to have your opinions of these statutes, and one addendum.

I am particularly concerned about the failure of the Congress to assert our constitutional prerogatives. When you have the President's wiretap program, there is a provision of Article I, section 8, which sets forth Congress' power. It is, "To make rules for the Government and regulation of the land and naval forces." And that is about as close as you can come in 1787 to authority to watch what the Government does on electronic surveillance. The Congress has been inert, really indifferent to the incursions on our constitutional authority. And we are caught in a squeeze with the Supreme Court where they declare our Acts unconstitutional because of our, quote, method of reasoning and a usurpation of super-legislative authority. And it is a regrettable situation that we spend much of our time debating lobbying and ethics and campaign finance, which are all important subjects, but not nearly as important as our constitutional responsibilities.

This Committee intends to be very vigorous in the pursuit of the electronic surveillance program. We are finding it hard to get traction on it, but we are going to keep trying. And we are going to be pursuing these statutes on disclosure, on this business about contempt for reporters. A contempt citation is different. Contempt citations for Judith Miller ended up in a longer jail term than most prosecutions.

Senator Leahy, I have exceeded my time, but in the absence of any other Senator here to watch the clock, it is like a tree falling in the forest.

Senator LEAHY. I share the concern. I share the concern that this Congress has done very little oversight. This has not helped—there are some who may think at the White House this helps by having a Republican-controlled Senate that refuses to ask questions of a Republican administration. I would argue otherwise. Just as it would not help a Democratic administration to have a Democratic-controlled House and Senate that did not ask them questions. Asking questions makes people better. Those of us who have to run for election or re-election, we know what that is like. We have to answer questions. This administration has been reluctant to, and I think it has hurt them.

I think it is also what is behind this new idea of just classifying everything willy nilly. We saw it at the Archives where historians suddenly find materials that they have had for decades. The move was being made to yank them out and classify them. Something that is on a website for weeks and weeks and weeks is suddenly classified just before—maybe it is coincidence, but just before a Congressional debate begins where we might refer to that website.

Even under the best of circumstances, it is difficult getting information from any administration. One of the reasons I support

FOIA is that administrations, Democratic and Republican, will tout their successes. Most don't want to tout their mistakes.

Mr. Chairman, you talk about sometimes getting the answers. As I recall, in the Intelligence Committee, when former Director of the CIA, Bill Casey, God rest his soul, came up for the third time in maybe a week or so to apologize to the Intelligence Committee because there was something that he was required by law to inform us of and had not. But he was there because even though nobody in the Congress had ever been informed of this, we read about it first in the newspapers. And then he would come up and say, "By the way, I meant to have told you about that" after somebody in the administration leaked it to the papers.

After the third time, I said, "You know, you are spending a lot of money to brief the Chairman, the Vice Chairman, every day someone comes from the CIA with a little package of classified material." I said, "Why don't you do this? Take the New York Times, mark it 'top secret,' and deliver that." I said, "We have three benefits: one, we will find out about these things a heck of a lot quicker than we do from you; second, we will find out in far more detail; and, third, there is that wonderful crossword puzzle."

He did not find it as amusing as one of the agents who was sitting behind him, who suddenly didn't find it amusing either when the Director turned around and looked at him.

Let me go to another question, I would hope when you are having discussions within the administration, no administration has ever spent so much money—it is now in the billions of dollars—to classify as much as this one has. Many of us are beginning to feel—and it is not just Democrats—many Republicans are beginning to feel that this is being done to cutoff criticisms of mistakes or open debate. And the Chairman said many, many times, we find out about things when we read them in the paper.

Now, you and I have talked a lot about getting a fully functional case management system in the hands of agents. Last year, after consultants pronounced it obsolete and riddled with problems, the FBI scrapped the $170 million Virtual Case File component of Trilogy. Now we are told that the Trilogy successor, Sentinel, will cost the American taxpayers an additional $425 million. But what bothers me even more, it will take 4 more years to deploy.

And then there is an article in U.S. News and World Report, which has often been very supportive of the administration. They suggest the Bureau may be skimming funds from other programs to help pay for Sentinel and hide its real price from Congress. According to the article, "some agents in the field have been told to use their cars judiciously, curtail use of informants, covert offsite rentals for undercover operations," and then "there is an increase in chatter that is as great or greater during VCF that Sentinel is going to fail."

Two questions. How confident are you in the FBI's current estimate for the Sentinel program, $425 million, 4 more years? And, second, are there other programs that have to be cut or scaled back to pay for Sentinel?

Director MUELLER. I am quite confident that we are on the right track with Sentinel for a variety of reasons: number one, the contractor, Lockheed Martin; second, it is a service-oriented architec-

ture, it is off-the-shelf products that we are using. And not only am I confident that we will move through the contract as we anticipated, but at the end of it, I think we will be far better off because we are—we will not be dealing with a proprietary system, but we will be dealing with a system of off-the-shelf products that can be continuously updated.

One of the reasons that it is taking 4 years is I want to make absolutely certain that each phase—and there are four phases—is it works and is beneficial to those to whom it is being provided. And if it fails in phase one, which I do not anticipate, then we are not down a course that we cannot rectify.

Let me turn for a second to the issue about whether or not we have been open with the funding on this. We have been absolutely open with the funding on both Virtual Case File and now Sentinel. What that article—

Senator LEAHY. Is there anything that is being cut or are there any other accounts that are being tapped?

Director MUELLER. Let me explain that in the year 2005, because we did not have a contract and yet we had to anticipate the funding for 2006, we put aside $97 million in a reprogramming that was approved by the Department of Justice. It was approved by OMF, and it was thoroughly briefed to the Hill and approved by the Appropriations Committee on the Hill.

Of that $97 million, approximately $73 million were redirected from no-year and prior year balances. There was a remaining $24 million in which a number of the divisions in the FBI contributed. And it is that shortfall that we had in order to bring in and utilize the $97 million in 2006, to which they may be referring. But all of this was—

Senator LEAHY. Would that $97 million be part of the $425 million today or in addition to the $425 million?

Director MUELLER. I believe it is in addition to—well, no, I don't think—I think it is part of the $425 million. I will have to check on that.

Senator LEAHY. Are we over half a billion or under half a billion?

Director MUELLER. It is part of it. It is part of it. It is part of the 425.

Senator LEAHY. Do you anticipate any programs being cut to pay for Sentinel outside the $425 million?

Director MUELLER. At this juncture, no, I do not.

Senator LEAHY. Will you notify us if they are?

Director MUELLER. Yes, absolutely. In order to move the funds, we would have to do a reprogramming. It would have to be approved by the Hill, which is what we did with the $97 million.

Senator LEAHY. Now, going into an area that Senator Feingold raised, on Friday the Justice Department reported that in 2005 the FBI delivered 9,245 national security letters for information on 3,501 U.S. citizens and legal residents. Now, that is the first time that the numbers have been released. Of course, Congress required it in the PATRIOT Act reauthorization, and I worked hard to get that requirement. The Justice Department had originally objected to that, although they gave no reasons why they should keep it classified.

The FBI was a lot more constructive in that discussion, and I want to thank you for that. You were far more open. We are not asking for ideatifying information, obviously, but the aggregate numbers don't give anything to any enemies. But it gives the American people a way to monitor the extent to which their Government is spying on them.

How does that 2005 number compare to past years? If you were to take a trend line for 10 years—

Director MUELLER. On NSLs, you are talking about?

Senator LEAHY. Yes.

Director MUELLER. I would think after September 11th it would be—and the passage of the PATRIOT Act, it would be a substantial increase.

Senator LEAHY. Would you support declassifying information about the number of NSLs issued since 9/11?

Director MUELLER. I'd have to look at the issue. I can't give an opinion at this point, Senator.

Senator LEAHY. Well, nothing was given away or hurt by disclosing last year's. Give me your thoughts on that.

Director MUELLER. I will. I can tell you that there would be a substantial increase. I mean, our mission has shifted dramatically since September 11th. That is what I understand. So—

Senator LEAHY. This is not a "gotcha" question. I am just curious about which way we are going, and, of course, I would expect a higher number after 9/11. But I would like to know how the trends are going.

Director MUELLER. Off the top of my head, I don't know what the trending is. I would say that is a very small number. When you talk—we have 300 million people in the United States now. It is a remarkably small number. I would say only—we only had that number. But I don't know the trending, and, again, it is an issue that I would have to think about, and quite obviously, the Department of Justice would have their thoughts on it.

Senator LEAHY. Thank you. We have a vote on, and I have gone beyond my time. You know, these annoying things, having votes, what in heaven's name do they expect Senators to do?

For anybody who is watching this back in Vermont, that is a joke.

[Laughter.]

Senator LEAHY. I consider it a great privilege and a great honor to be able to vote. Last month, I became the 12th person in history to cast 12,000 votes. Some of my colleagues on the other side of the aisle said out of 12,000 I got three or four right. Thank you.

Chairman SPECTER. Director Mueller, thank you very much for coming in today.

Director MUELLER. Thank you, Senator.

Chairman SPECTER. We appreciate your service. We know the responsibilities. There is a lot of concern about the new system for recordkeeping, using the up-to-date techniques. It is problemsome that it will not be online fully operational for a very protracted period of time. But I like the idea of your sitting down with the contractors on a periodic basis. You have got a lot at stake there, and there have been a lot of problems, and you are not a magician. We do not hold you responsible for the problems you have had, but to

get it done and get it done right is really important so you can function, you can have the information within your Bureau, and share the information with others.

You have the PATRIOT Act, and we are concerned about the scope of the authority that you have, and we will have oversight hearings on it. We find those most productive. But what I would like to know—and we will be calling for some closed sessions—is what have these tools given you? What have these national security letters enabled you to find out? What have you been able to learn from the authority to get business records? Are you being unduly restricted by what we have put into the Act? Because the fight against terrorism is so very, very important. And we understand that you do not make decisions on the electronic surveillance program. I have not asked you any questions about that because I do not expect you to provide any answers on the subject. And the administration position on enforcement of these laws is not precisely your bailiwick, but it is close enough so that I think it is appropriate to ask you those questions. And you do conduct the investigations, and your agents are on the spot, and your agents are interviewing all these people for the grand jury. You are in the middle of these cases. You are not the prosecutor, but you are pretty close. You are pretty close to the prosecutor. And you have very heavy responsibilities on protection of civil liberties as well. And we are about to come to the Voting Rights Act, which gives you a lot of authority and a lot of important responsibility.

So we thank you for coming in, and may the record show that we are letting you go about 20 seconds before noontime.

Director MUELLER. Thank you, sir.

Chairman SPECTER. We have a vote. We have a second panel, and we will return shortly to proceed. Thank you.

[Recess at 12 noon to 12:27 p.m.]

Chairman SPECTER. We have delayed the appearance of Panel Two, but you have been here for the last 3 hours, so you know exactly what is going on.

Your testimony is very important, and it is regrettable, but it is hard to round up Senators after votes. It just is. But your testimony will be reviewed, I am sure, by other members of the Committee and staffs.

We turn first to the Inspector General of the Department of Justice, Glenn A. Fine. He has been serving in that capacity since August of 2000, although was acting Inspector General for a time. He has an outstanding academic record, magna from Harvard College, Rhodes scholar, master's degree from Oxford, and a law degree, again, magna cum laude from Harvard Law School. Why weren't you named Chief Justice?

[Laughter.]

Chairman SPECTER. We will put in the record his curriculum vitae, which is outstanding, and we thank you for the work you are doing in this very important position, and the floor is yours for 5 minutes.

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

General FINE. Mr. Chairman, thank you for inviting me to testify about the OIG's oversight work related to the FBI. The OIG has devoted extensive resources to reviewing FBI programs and operations at the FBI as it continues its transformation after the September 11th attacks.

When assessing the FBI, I believe it is important first to acknowledge the dedication of its employees. The FBI attracts patriotic individuals who are committed to the FBI's important mission. These employees deserve recognition for the sacrifices they make in carrying out their critical responsibilities.

Their task is difficult, and the FBI is under regular and probing scrutiny by Congress, the OIG, and other oversight entities. That is as it should be. Given the importance of its mission and the impact the FBI has on safety, security, and civil rights in the United States, such scrutiny is warranted. I have found that its leaders, particularly Director Mueller, understand the value of such independent oversight.

In general, I believe the FBI has made progress in addressing some of its critical challenges, but more progress is clearly needed. The first area where additional progress is needed is the ongoing effort to upgrade the FBI's information technology systems. For too long the FBI has not had the modern IT systems it needs to perform its mission as efficiently and effectively as it should. The FBI's failed Virtual Case File effort was a major setback in both time and money in the FBI's urgent need for IT modernization.

The FBI's current project to upgrade its information technology, Sentinel, appears to be on the right track. However, we have identified several issues the FBI needs to address as it moves from preacquisition planning to development of Sentinel. The OIG plans to closely monitor the Sentinel project, and we will raise any concerns with the FBI and this Committee as the project moves forward.

A second challenge for the FBI is to pursue its law enforcement and intelligence-gathering missions while at the same time safeguarding civil rights. The OIG has performed various reviews related to civil rights issues, including a review of the FBI's compliance with Attorney General guidelines, a review of intelligence violations forwarded to the President's Intelligence Oversight Board, and a review of the FBI's interviews of protesters connected to the 2004 Democratic and Republican National Conventions, which Director Mueller mentioned earlier today. Currently, we are reviewing the FBI's use of national security letters and orders for records under Section 215 of the PATRIOT Act.

A third challenge for the FBI is to recruit, train, and retain skilled individuals in critical positions, such as intelligence analysts, linguists, and information technology. Moreover, the FBI has continuing turnover in key management positions at FBI headquarters and in the field. In my view, rapid turnover in these positions reduces the FBI's effectiveness.

Fourth, in large part the FBI's success depends on its ability to share information, both internally within the FBI and externally with its Federal, State, and local partners. Without effective infor-

mation sharing, the FBI's counterterrorism, counterintelligence, and criminal investigative efforts are diminished.

Fifth, while there is little dispute that the FBI must transform itself to place counterterrorism as its highest priority, the FBI cannot neglect other criminal investigative areas where it has a unique role to play. The FBI's allocation of investigative resources needs to be continually monitored to ensure that important areas are not neglected.

Sixth, as the Robert Hanssen case demonstrated so tragically, the FBI must remain vigilant in its internal security and counterespionage efforts. The FBI can never afford to become complacent about the continuing threat of espionage from both inside and outside the FBI. The OIG is now conducting a follow-up review to assess the FBI's progress in improving its internal security since the Hanssen case.

And, seventh, the FBI is a leader in a variety of forensic science disciplines, but mistakes in the FBI laboratory can have dramatic consequences, as demonstrated by the laboratory's fingerprint misidentification in the Brandon Mayfield case. The FBI must be vigilant to ensure that the laboratory is not vulnerable to mistakes or willful abuse.

My written statement discusses in more detail many OIG reviews in these areas. In sum, our reports have found that while the FBI has made progress in addressing its changed priorities since the September 11th terrorist attacks, significant challenges and deficiencies remain. These are not easy challenges, and they require constant attention and oversight. To assist in these challenges, the OIG will continue to conduct vigorous oversight of FBI programs and provide our recommendations for improvement.

That concludes my prepared statement, and I would be glad to answer any questions.

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

Chairman SPECTER. Thank you very much, General Fine. And thank you for concluding almost on the button.

We now turn to Ms. Linda Calbom, the Government Accounting Office's Western Regional Director and the author of the report. She is a summa cum laude graduate from Washington State University. Mr. Fine was magna. She is summa.

Ms. CALBOM. You beat me.

Chairman SPECTER. Mr. Gannon, that puts a very heavy burden on you.

Mr. GANNON. Can I leave now?

[Laughter.]

Chairman SPECTER. I had Latin, and I don't know where we are going from here. We will put her extensive resume in the record, but we will note also that she spent 11 years in public accounting with Deloitte and Touche in Seattle, Washington, so she comes to this position with impeccable credentials. Thank you for joining us today, Ms. Calbom, and we look forward to your testimony.

STATEMENT OF LINDA M. CALBOM, DIRECTOR, FINANCIAL MANAGEMENT AND ASSURANCE, GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, D.C.

Ms. CALBOM. Thank you very much, Mr. Chairman, and thank you also for the opportunity to discuss our report that we recently issued. And, of course, it was developed at the request of this Committee, and this report is on the results of our audit of FBI's internal controls over contractor payments and equipment purchases related to the Trilogy project.

Also with me today is Eileen Larence, who is one of the Directors responsible for our report on information sharing, so she will be available to answer any questions you may have on that report.

But today I wanted to summarize the results of our work with respect to, first, weaknesses in FBI's internal controls that made it vulnerable to improper payments of contractor costs; second, payments for questionable contractor costs that we identified in our audit; and, third, FBI's inadequate accountability for assets that it purchased with Trilogy project funds.

First of all, FBI's review and approval process for the Trilogy contractor invoices, which was actually carried out by a team consisting of FBI, GSA, and Mitretek, did not provide an adequate basis to verify that goods and services billed were actually received by FBI or that amounts billed were appropriate. This occurred in part because the responsibility for the review and approval of the invoices was not really clearly defined or documented amongst the parties.

In addition, contractor invoices frequently lacked the types of information necessary to validate the charges. For example, we have a slide—and, Mr. Chairman, I think in front of you is a sheet that shows an example here; of an invoice that has a lot of details about the small charges, but no details at all for the $1.9 million charge that made up the lion's share of the bill.

Despite this, this invoice, and many others like it, were paid without requesting additional supporting documentation. These weaknesses in the review and approval process made FBI highly vulnerable to the payment of improper contractor costs. In order to assess the effect of these vulnerabilities, we used forensic auditing techniques to select certain contractor costs for review. As shown in the next slide, which I think you have up there as well, Mr. Chairman, we found about $10.1 million of questionable contractor costs paid by FBI. These costs included payments for first-class travel and other excessive airfare costs, incorrect billings for overtime hours, overcharged labor rates, and inadequately supported subcontractor labor and other direct costs.

Given FBI's poor control environment over invoice payments and the fact that we reviewed only selected FBI payments to Trilogy contractors, other questionable costs may have been paid for that were not identified. Our audit also disclosed that FBI did not maintain accountability for equipment purchased for the Trilogy project. FBI relied extensively on contractors to account for Trilogy assets while they were being purchased, warehoused, and installed. However, FBI did not establish controls to verify the accuracy and completeness of contractor records that it was relying on.

Moreover, once FBI took possession of the Trilogy equipment, it did not establish adequate physical control over the assets. Consequently, we found that FBI could not locate over 1,200 assets purchased with Trilogy funds which were valued at approximately $7.6 million.

While we are encouraged by FBI's current efforts to account for these assets, its ability to definitively determine their existence has been compromised by the numerous control weaknesses identified in our report. Further, the fact that assets had not been properly accounted for at the time of our review means that they were at risk of loss or misappropriation since being delivered to FBI. In some cases, that was several years.

Our report includes 27 recommendations to address the issues that we identified in our audit, and I am pleased to say that FBI has been receptive to our recommendations and has begun to take actions to implement them. But let me just emphasize the importance of continuously monitoring the implementation of corrective actions to ensure that they are effective in helping to avoid the same type of pitfalls that occurred with the Trilogy project. Without such monitoring, Sentinel and other IT efforts will be highly exposed to the same types of negative outcomes that they experienced with Trilogy.

That concludes my prepared statement, Mr. Chairman.

[The prepared statement of Ms. Calbom appears as a submission for the record.]

Chairman SPECTER. Thank you very much, Ms. Calbom.

Our final witness on the panel is Dr. John Gannon, Vice President and Senior General Manager for Global Analysis at BAE Systems, Inc. He has a bachelor's degree in psychology from Holy Cross, an MBA and Ph.D. from Washington University, St Louis, and is an adjunct professor in the National Security Program at Georgetown. He has an extraordinary list of awards: the President's National Security Medal, the CIA's Distinguished Intelligence Medal, the CIA's Director's Medal. And we will put into the record a full list of his outstanding record.

We have had a lot of panels up here before this Committee. I do not think we have had one with the credentials that you three bring.

Thank you, Mr. Gannon, for joining us, and the floor is yours for 5 minutes.

STATEMENT OF JOHN C. GANNON, VICE PRESIDENT FOR GLOBAL ANALYSIS, BAE SYSTEMS INFORMATION TECHNOLOGY, AND FORMER STAFF DIRECTOR, HOMELAND SECURITY COMMITTEE, U.S. HOUSE OF REPRESENTATIVES, MCLEAN, VIRGINIA

Mr. GANNON. Thank you, Mr. Chairman. Thank you for the opportunity to participate this morning in this important hearing. I have great respect for the Bureau as a Federal law enforcement agency, and strong admiration for FBI officers with whom I have worked over the years. FBI officers are working hard today in the most challenging environment they have ever faced under an able Director of legendary energy, dedication and integrity.

The views expressed now and in my longer written statement for the record are my own. They are shaped by my professional experience working with the FBI during a 24-year career at CIA, during a brief stint as a team leader for intelligence in the Transition Planning Office for the Department of Homeland Security, and during a 2-year tour as the first staff director of the House Homeland Security Committee. The also are influenced by my long experience building and managing analytic programs in the intelligence community, where I served as CIA's Deputy Director for Intelligence, as the Chairman of the National Intelligence Council, and as Assistant Director for Analysis and Production.

I would make four points to you, sir, today. First, the FBI, as I have observed it, has made progress in intelligence, but I think it is important for us to distinguish between the Bureau's traditional law enforcement mission and its new national intelligence mandate. In the first instance, I believe the FBI is increasingly using intelligence collection and analysis, including in its new field intelligence groups, against the increasingly complex issues associated with its criminal investigation mission. The Bureau should be encouraged in this path. Intelligence that benefits a special agent in charge can also be useful at the national level.

But second, the FBI is unacceptably behind, however, in developing a national intelligence collection and analytic capability. The Bureau has not structured an intelligence collection requirements process that legitimate consumers can readily tap, and it is not, to my knowledge, producing on any predictable basis authoritative assessments of the terrorist threat to the homeland. These are serious gaps. It is a good thing that the Bureau's law enforcement culture is being enriched by intelligence. It is not a good thing that law enforcement continues to trump intelligence in the effort to build a domestic intelligence capability. The status quo, in my view, is not acceptable.

Third. Even if the FBI were doing better on this domestic intelligence mission, I believe we would find that the mission in today's information environment is much bigger than the FBI and well beyond its resources and competence to carry out. Domestic intelligence today is about protecting the U.S. homeland from threats mostly of foreign origin. It does involve the FBI's law enforcement and counterterrorism work, but it relates more to the establishment of a national intelligence capability, integrating Federal, State and local government, and when appropriate, the private sector, in a secure, collaborative network to stop our enemies before they act, and to confront all those adversaries capable of using global electronic and human networks to attack our people, our physical and cyber infrastructure, and our space systems. These adversaries include WMD proliferators, terrorists, organized criminals, narcotics traffickers, human traffickers, and countries, big and small, working alone or in combination against U.S. interests.

I see the FBI on its present course as a contributor to this vital effort, but not as the leader of a new model of collaboration in the information age.

Fourth. Domestic intelligence, moreover, must be viewed as an integral part of U.S. intelligence community reform. The connection between foreign and domestic intelligence must be seamless today

because the threats we face know no borders. The challenge is Government wide, has historic roots that long precede 9/11, and must be concerned, as I have suggested, with a range of deadly threats to our National security, largely from abroad and not restricted to international terrorism. The domestic piece must be an essential part of the transformation of U.S. intelligence driven by the Director of National Intelligence, the Secretary of Defense, the Attorney General, and the Secretary of Homeland Security.

That coordinated effort today, which in my view, needs stronger sustained direction from the White House and the Congress, should be moving as a top priority to unify strategies, to clarify roles and responsibilities across competing agencies, and to reduce the IC's bloated bureaucracy, which is today larger than ever.

Thank you, Mr. Chairman. I would be glad to take questions on what I have said or on the longer statement that I have made for the record.

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

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

Mr. Fine, the role you have as Inspector General for the Department of Justice is a very, very important role, and I have personally been very pleased to see the work that the Inspectors General do generally. During the time I chaired the Intelligence Committee, I took the lead—really, my staff director, Charles Battaglia took the lead—so often when leads are taken by Senators, they are really staff leads—in establishing the Office of Inspector General for the CIA. We almost lost the bill because of that provision, President Bush being an ex-CIA Director, but we got it through. So I have seen the work that the Inspectors General do.

The initial thought which comes to my mind is whether you could exert your authority to review the electronic surveillance program, or perhaps I ought to begin and ask if you have reviewed the program for constitutionality?

General FINE. We have not done that. That issue has to do with the legal authority for the program, and quite unfortunately, in my view, the jurisdiction of the Inspector General in the Department of Justice is limited to some degree because there is a Department of Justice Office of Professional Responsibility that has jurisdiction to review the actions of attorneys in the exercise of their legal authority up to and including the Attorney General. To my knowledge, the Department of Justice is the only area where the Inspector General's Office has that limitation on its authority, and so—

Chairman SPECTER. Where does that limitation arise from, Mr. Fine?

General FINE. It originally arose from Attorney General orders issued by Attorney General Reno and Attorney General Ashcroft, and it was codified in the DOJ Reauthorization Act by the Congress. So it would require a Congressional action to change it at this point, but it is a limitation on our authority that does not exist, to my knowledge—

Chairman SPECTER. What does it say specifically to limit your authority?

General FINE. That the Inspector General has authority throughout the Department of Justice except for the actions of attorneys

in the exercise of their authority to litigate, investigate or provide legal advice. And so that has been a carve-out. The Department of Justice's Office of Professional Responsibility existed before the Inspector General's Office was created in the Department of Justice. We were created in 1989, and that limitation on our authority has continued to exist.

Chairman SPECTER. You say that the Office of Professional Responsibility has the authority to review what the lawyers do?

General FINE. Correct.

Chairman SPECTER. Has there been an inquiry by that office in the propriety of the opinion of the Department of Justice of holding the constitutionality of the electronic surveillance program?

General FINE. Yes. My understanding is the Department's Office of Professional Responsibility has been looking into that issue and is conducting a review of that matter.

Chairman SPECTER. What is their basis for their doing that?

General FINE. Because it revolves around the actions of the Department of Justice attorneys in providing legal authority for the—

Chairman SPECTER. Well, I know they did that, but was there some predicate, some reason to conduct the investigation that you know of?

General FINE. Yes. There was a request from several members of the House of Representatives to conduct that kind of investigation. It was sent to us. It was referred to the Office of Professional Responsibility. They agreed to do that.

Chairman SPECTER. But ordinarily you need a predicate, you need some reason to conduct an investigation. Was any given?

General FINE. There were questions about the authority and the legal opinion concerning that. And quite honestly, we often investigate things on our own when we see an issue that needs to be resolved, and I believe the Department of Justice saw—

Chairman SPECTER. When you investigate things on your own, you ordinarily have a reason.

General FINE. Correct.

Chairman SPECTER. Was the House acting on the newspaper reports about the reported meeting in the hospital with the Attorney General and the Deputy and Chief of Staff?

General FINE. I think the House was acting on the information that came out in the press regarding a surveillance program. And when that information arose, they sent the request.

Chairman SPECTER. Mr. Fine, there was an issue raised on your prior testimony, Mr. Fine, on making suggestions to the FBI. Have you done that?

General FINE. I am sorry, Mr. Chairman?

Chairman SPECTER. There was an issue raised. I had a hearing in July of 2005 about your feeling free to make affirmative suggestions to the FBI as well as performing your role as a constructive critic. Have you made suggestions?

General FINE. Yes, absolutely. In almost all of our reviews, not only do we look backward and see what went wrong, but we try to make recommendations to improve operations and improve programs. And we follow-up through the FBI to resolve those issues, and sometimes we even open follow-up reviews to see whether they have actually implemented the changes that we made.

For example, we opened a follow-up review recently about the FBI's hiring, retaining and training of intelligence analysts. We made recommendations in a report several years ago. We want to see what progress they have made.

Chairman SPECTER. Mr. Fine, the staff has prepared six tough questions for you which I do not have time to ask you, but they will be submitted to you, and we would like you to answer them for the record.

General FINE. I would be glad to do that, Mr. Chairman.

Chairman SPECTER. Ms. Calbom, you have noted that you have made 27 recommendations. How many has the FBI implemented?

Ms. CALBOM. We have not yet gone back in to look and see what recommendations they have or have not implemented. As part of our normal followup on any report, after some times has gone by, and particularly after we get their 60-day letter that they are required to respond back formally on their actions taken to implement our recommendations, then we will be going through a process where we will look at the actions that they have taken.

Chairman SPECTER. So you will take a look to see how many they have implemented.

Ms. CALBOM. Yes, we will.

Chairman SPECTER. Would you report back to us, if they do not implement them all, and tell us how many they have implemented, how many they have not?

Ms. CALBOM. We certainly can do that, Mr. Chairman.

Chairman SPECTER. We would like to know that. You are going to continue your reporting on the Trilogy program and the Sentinel program to see if this money is being well spent. Here again, I cannot go into all these questions, but there are a series of very piercing questions which I would like to submit to you to have your answer for the record. But let me emphasize the need for you to keep a close watch on that program. It is going to take a lot of surveillance. The Director has committed to periodic review, but it is going to take more than that. Are you in a position to followup on that?

Ms. CALBOM. We have not received any formal request yet to do that, but certainly when we do, we are in a position to do that, Mr. Chairman.

Chairman SPECTER. My request is not sufficiently formal?

Ms. CALBOM. It is now, yes, sir.

[Laughter.]

Chairman SPECTER. Well, that is true, you said you hadn't, you did not say you haven't.

Mr. Gannon, how well is the new Director of National Intelligence working out?

Mr. GANNON. In some ways, I think there are some things being done. In other ways—

Chairman SPECTER. Let me be specific. Has he taken command?

Mr. GANNON. I would prefer to see a larger profile—

Chairman SPECTER. Prefer to see what?

Mr. GANNON. I would prefer to see a larger profile and a stronger direction.

Chairman SPECTER. What is he not doing that he should be doing?

Mr. GANNON. Partly some of the issues that I addressed in my opening statement. I think there is a real need to establish roles and responsibilities with regard to the Department of Defense, with regard to FBI. I talked somewhat critically about FBI, but what is the direction being given to FBI with the authorities that the DNI has?

Chairman SPECTER. The Department of Defense is moving into these fields with a widespread expansion of powers. Is that consistent with having a Director of National Intelligence?

Mr. GANNON. I think what is bothersome is that movement that you are talking about is taking place without any supervision beyond the Department of Defense, and I think it is needed, from the DNI, but also from the White House.

Chairman SPECTER. Doesn't the DNI have authority over the Department of Defense on intelligence matters?

Mr. GANNON. I think it is not entirely clear on some issues, but I think he has more authority than I am seeing exercised.

Chairman SPECTER. What are you saying, that he would have to invade the Pentagon in order to establish his authority?

Mr. GANNON. No. I would say that you have to claim your jurisdiction you have, and seek jurisdiction that you might not have.

Chairman SPECTER. An invasion would not be necessary?

Mr. GANNON. Right.

Chairman SPECTER. But helpful.

Mr. GANNON. And I think that is partly because the legislation does not make clear what authority he does have.

Chairman SPECTER. Perhaps you have already done it, but we would be interested in a more precise analysis on that issue, as to where the Department of Defense is going. We note your emphasis on the Department of Homeland Security as having primacy. You think they should have primacy over the FBI, right?

Mr. GANNON. No, sir, I did not put it that way, and in my written statement, I do have quite a lot to say about the Department of Defense in the longer statement. But what I did say was that in the domestic intelligence collection, I think the model that we should be pursuing is a collaborative one, not a centralized new intelligence service or one that would make FBI what I do not think it can be, in that as a centralized—

Chairman SPECTER. I have written questions for you too, and one of them identifies your written testimony to push DHS into the lead role.

Mr. GANNON. That is one. I offered two options. One is that if you want the FBI to be the leader of the domestic intelligence effort, there has to be some major restructuring done there that is not being done. You cannot get there from the path that FBI is on now.

The other option is to reinvigorate, almost go back to the Homeland Security Act of 2002, and give the Department the authorities that it was supposed to have under that legislation. Then I think because it is a department that is designed really to build a collaborative model, it would be the integrator of the information and intelligence, and FBI would be a contributor, but the department would not control the FBI.

Chairman SPECTER. Is the collaboration and integration adequate?

Mr. GANNON. I think in our society, I think the design of a system that is collaborative and not centralized as an intelligence service is, I think, the best model for our society as I see it and understand it.

Chairman SPECTER. I do not understand your answer. Is the collaboration and integration adequate, satisfactory?

Mr. GANNON. Oh, today?

Chairman SPECTER. Yes.

Mr. GANNON. Oh, absolutely not. I thought you meant is it in the model. No, absolutely not today.

Chairman SPECTER. Well, would you—we are going to submit these questions to you, but add an additional one for me. What specifically ought to be done to make it collaborative and integrated?

Mr. GANNON. Sure.

Chairman SPECTER. I really regret that there are not more Senators here to hear your testimony. But that is an inevitable fact of life. Everybody has many committees and many subcommittees, and frequently you are stuck with just the Chairman, but we have your reports, and we have your written testimony. And these questions are unusually good questions that I have reviewed that we will ask you to respond to for the record. They are so good that I am going to identify the staffers who worked on this hearing: Josh Latarette, Kathy Michalko, Adam Turner, Dallas Kaplan, Adam Caudle, Evan Kelly and Matt McPhillips. I will not identify who wrote them down because I may have misstated some of the names because the printing is not really legible.

[Laughter.]

Chairman SPECTER. We have had some interjections from the peanut gallery, from the stands.

These are really enormously important subjects as to how we get the FBI systems, in effect, with the high price on them noted. Somebody estimates it at a billion dollars. Very important how the system is working, and that the Department of Defense fit into the picture with the Director of National Intelligence. It has been a long time getting there. I worked on that, the Governmental Affairs Committee. We took time off from the summer of 2004, took time away from a campaign for reelection it was so important. That is pretty hard to do in August to come back. We had special hearings, and I drafted a bill on it, and others did too, and we finally put that into place. But unless it is implemented, it is worthless.

So your supplemental ideas on how to accomplish that are very important, and we greatly appreciate them. Without objection, I am

going to make a copy of the letter from Attorney General Ashcroft a part of the record.

Let me express some regrets, that I had not known that we were codifying the Attorney General's limitation of the Inspector General's authority. It does not seem to me that the person to be inspected ought to have the standing to limit the inspector's authority. But then somehow, if it is codified—there is a lot codified that does not have any Congressional intent behind it. Justice Scalia is right about that.

Thank you all very much. That concludes our hearing.

[Whereupon, at 1:02 p.m., the Committee was adjourned.]

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

QUESTIONS AND ANSWERS

United States Government Accountability Office
Washington, DC 20548

June 9, 2006

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate

Subject: *FBI Trilogy: Responses to Posthearing Questions*

Dear Mr. Chairman:

This report responds to your request for additional information related to the committee's May 2, 2006, hearing entitled *FBI Oversight*. Enclosed are our responses to the supplemental questions you submitted for the record. Our responses are based largely on information contained in our published report, entitled *Federal Bureau of Investigation: Weak Controls over Trilogy Project Led to Payment of Questionable Contractor Costs and Missing Assets*, GAO-06-306. As discussed in my statement at the hearing, unless the Federal Bureau of Investigation (FBI) strengthens its controls over contractor payments and purchased equipment, future projects, including the new Sentinel project, will be highly vulnerable to same types of issues that plagued the Trilogy project.

If you have any further questions or would like to discuss any of the issues in more detail, please call me at (202) 512-8341. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

Sincerely yours,

Linda M. Calbom

Linda M. Calbom
Director
Financial Management and Assurance

Enclosure - 1

Enclosure

Responses to Written Questions for the Record Submitted by Chairman Arlen Specter, Committee on the Judiciary, on *FBI Oversight* Hearing, May 2, 2006

1. **In your February Trilogy report, you offered the FBI a number of recommendations to "(1) facilitate the effective management of interagency contracting, (2) mitigate the risks of paying potentially unallowable or questionable costs in connection to cost-reimbursement type contracts, and (3) improve FBI's accountability for and safeguarding of its computer equipment." Has the FBI implemented your recommendations?**

Answer:

We will be following up on FBI's efforts to implement our recommendations as part of our normal tracking and evaluation process for open recommendations. This process begins with our receipt of a copy of FBI's formal written response to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Government Reform on its plans to implement our recommendations, which is due 60 days after our report is publicly released. We received a copy of this formal response letter on May 30, 2006.[1] In addition, at the request of this committee, we will evaluate FBI's internal controls over contractor invoices and asset accountability for the Sentinel project—the FBI's new electronic information management system initiative—to help ensure that the internal control failures we identified with Trilogy are not repeated. After we have completed this follow-up work, we will report to you on our assessment of FBI's actions to implement our recommendations.

2. **In testimony before the House Appropriations Subcommittee on Science, State, Justice, Commerce and Related Agencies on March 28, 2006, Director Mueller told the panel that GAO will be auditing the Sentinel**

[1] FBI's letter was dated May 12, 2006.

program. What measures will you be taking to ensure that the same mistakes from the Trilogy debacle are not repeated?

Answer:

In reference to Director Mueller's comment, GAO is currently reviewing the Sentinel program at the request of the Chairman and Ranking Minority Member of the House Committee on the Judiciary. In this review, GAO is examining the program's (1) use of effective methods for acquiring commercial solutions, (2) efforts to align itself with the bureau's enterprise architecture, (3) basis for reliably estimating costs and schedules, (4) plans for applying earned value management, (5) provisions for adequate human capital to manage the acquisition, and (6) relationship to the governmentwide case management line of business. This work is being coordinated with the Department of Justice Office of Inspector General and collectively should help determine whether the Sentinel project is being effectively managed. This work and the follow-up work described in our answer to question one will provide information on key aspects of FBI's efforts to ensure that the Trilogy mistakes are not repeated with Sentinel.

3. **In the Trilogy report, you reported a number of issues that perplexed this Committee. For example, 1205 pieces of equipment, worth an estimated $7.6 million, went missing—some of which were classified or secured computers. The project was overbudget and overdeadline, and around $10 million was wasted. Which of the issues that led to the delinquency of the Trilogy project did you find to be the most alarming? Is that issue still of concern to you? How has the FBI addressed it?**

Answer:

We reported on two fundamental issues that we consider to be key contributors to the problems we identified with the Trilogy project. First, the review and approval process for Trilogy contractor invoices did not provide an adequate basis for verifying that goods and services billed were actually received by FBI or that the amounts billed were appropriate. Second, FBI did not have an adequate process to ensure physical and financial accountability of assets purchased with Trilogy project

funds. In addition, we were unable to determine if any of the missing assets contained confidential or sensitive information and data. Therefore, we recommended that FBI further investigate those missing assets to determine whether any confidential or sensitive information and data may be exposed to unauthorized users.

We understand that FBI is taking actions to implement our recommendations to resolve the fundamental issues we identified. We will evaluate FBI's corrective actions as part of our normal recommendation follow-up process and during our review of the Sentinel project. Until corrective actions are fully implemented, both of these internal control issues will be a concern with Sentinel and other information technology projects at FBI.

4. **In your testimony, you discuss that FBI could not locate 1,404 [pieces of equipment]; you adjusted the number to 1,205 when you were able to verify that the FBI had found 199 pieces of equipment. However, in its response to your report, FBI stated that it had accounted for around 800 of the remaining items [of equipment]. Are you satisfied with the FBI's efforts to track these assets? Has the FBI given any explanation for the remaining roughly 400 assets that are completely unaccounted for?**

Answer:

In February 2006, FBI informed us that the approximately 800 remaining items, referred to above, that it believes it has now accounted for included (1) accountable assets[2] not in FBI's property system because they were either incorrectly identified as nonaccountable assets or mistakenly omitted, (2) defective equipment that was never recorded in the property system and was subsequently replaced, and (3) nonaccountable assets or components of accountable assets that were incorrectly bar coded. However, because FBI was not able to provide us with any evidence, such as location information, to support that it had actually accounted for these 800 assets, we could not definitively determine whether FBI had located these items. We

[2] According to FBI policy, assets valued at $1,000 or more, as well as certain sensitive items, such as firearms, laptop computers, and central processing units, are considered "accountable" assets, regardless of cost, and must be accounted for individually in FBI's property system.

considered these same issues during our audit in an effort to determine if assets were missing or merely miscoded.

The FBI also has not provided any additional explanation for the remaining roughly 400 missing assets. The numerous control weaknesses identified in our report are major factors contributing to FBI's continuing inability to find and definitively confirm the existence of these assets. Further, the fact that assets have not been properly accounted for to date means that they have been at risk of loss or misappropriation without detection since being delivered to FBI—in some cases, for several years. We will continue to monitor FBI's progress on locating these assets as part of our review of FBI's implementation of corrective actions to address our recommendations.

(190150)

Senator Specter
FBI Oversight Hearing
May 2, 2006

QUESTIONS FOR GLENN FINE

1. In your written testimony, you state OIG is auditing the Sentinel contract with Lockheed Martin to determine if it contains the "necessary work, requirements, benchmarks, and other provisions to help ensure the success of the project." When do you anticipate having this audit complete?

In March 2006, the OIG released the first in a series of audits that monitor the FBI's development and implementation of Sentinel, the successor to the $170 million Virtual Case File project that the FBI ended unsuccessfully after 3 years. This OIG review assessed the FBI's pre-acquisition planning for Sentinel, including the approach, design, cost, funding sources, time frame, contracting vehicle, and oversight structure.

In April 2006, the OIG initiated its second audit of the Sentinel project that will examine the $305 million contract recently announced with Lockheed Martin. This audit will attempt to determine, among other things, if the FBI has established the necessary work requirements, benchmarks, and other provisions to help ensure the success of the project. In addition, this ongoing review will assess the FBI's progress in addressing the recommendations made in the OIG's first Sentinel review.

We intend to complete and issue our second report on the FBI's Sentinel case management project before the end of calendar year 2006.

2. A June 2005 OIG report entitled "A review of the Terrorist Screening Center" found that the watch list could be missing names, some names might be designated at inappropriate threat levels and that the FBI hasn't given other agencies full access to its watch list. What steps has the FBI been taking to deal with this problem?

During our audit resolution process, the Terrorist Screening Center (TSC) reported that records found during our audit to have been excluded from the Terrorist Screening Database (TSDB) have since been reviewed and, if appropriate, have been included in the database. In addition, the TSC provided evidence during the resolution process to support its implementation of a new version of the database that automates the daily upload of records nominated for inclusion into the TSDB, therefore reducing missing watch list records.

The TSC also has provided us information regarding its ongoing review of the database to ensure that the information within it is complete, accurate, and non-duplicative.

With respect to the inappropriate handling codes (referred to as "threat levels" in the question above), TSC personnel provided documentation that they performed a review of database records against the TSC's nomination criteria to ensure the records are designated at the appropriate handling levels. This review resulted in the reassignment of handling codes for more than 50,000 records.

Finally, the TSC reported that it has provided access to the consolidated watch list, with any appropriate safeguards, to all of the end users identified in our report. In addition, the TSC has indicated that regular private-sector screening is anticipated in the future because the Department of Homeland Security, which is responsible for such screening, was in the planning stages for screening individuals at certain high-risk infrastructure facilities, such as power plants, at the time of our audit.

3. At our last FBI oversight hearing in July 2005, we talked about the importance that you feel free to make affirmative suggestions to the FBI as well as performing your role as critic. Have you been able to perform that role effectively and has the FBI been receptive to your suggestions?

Yes, I believe the OIG has been able to perform that role effectively. In almost all of our reports, we not only describe any problems we find with a program, we also provide recommendations to attempt to improve the program in the future.

The FBI generally has agreed with recommendations made by the OIG in our reviews, and it reports to us the corrective action it intends to take. We follow up on the resolution of our recommendations and ask for evidence that the FBI has taken the corrective action. In some cases, we also conduct a follow-up review to assess what progress the FBI has made in response to the recommendations in our initial review.

4. A *U.S. News and World Report* article entitled "High tech's High Stakes at the FBI" (U.S. News & World Report, 4/17/06), states "Some executives believe the bureau's computer upgrades (i.e. Sentinel) could ultimately total a billion dollars--double the projected costs ... at the bureau, tensions are rising as many officials stew over what they view as prudent across-the-board cost cutting to hide Sentinel's

***real* price tag from Congress and spare Mueller further ignominy." Including the costs of transferable assets from VCF, what is the total cost of Sentinel?**

We currently are evaluating the FBI's stated estimate that it will cost $425 million to develop and deploy the Sentinel system, and we are attempting to determine if there are other costs associated with the project that are not included in the FBI's estimate. This evaluation will be a part of the report discussed in response to question number one. We also will continue to monitor Sentinel's costs in future audits as the different phases of Sentinel are implemented.

5. The March 2006 OIG report on the FBI's efforts to protect the nation's seaports indicated that there were some coordination issues that needed to be addressed. The report indicates that potential jurisdictional and coordination issues between the UCCG and the FBI (who share incident response responsibilities) could be resolved by the passage of a final Maritime Operational Threat Response Plan (MOTR). In the area of seaport security, what should FBI be spending their energy on? What's most important?

We believe that the FBI and Coast Guard need to reach an understanding of incident command and control and how each agency should respond in a variety of scenarios. Both agencies also should conduct joint exercises so that these roles and responsibilities are well understood by employees of both agencies. The FBI also must work to gather better intelligence regarding the threats and risk level relating to maritime terrorism. Improving the FBI's intelligence relating to maritime and other potential terrorist operations may prove to be its most important challenge, because this intelligence will aid in the prevention of potential attacks.

6. How integral a role did the OIG play in the awarding of the Sentinel contract, and is your office convinced that the time schedule set forth is realistic and attainable? Will OIG continue to audit the Sentinel project to ensure the mistakes highlighted by the February GAO report are not repeated?

The OIG did not play a direct role in the Sentinel contracting process. However, the OIG has conducted reviews of the FBI information technology processes, such as our reviews of the Trilogy IT project and the failed Virtual Case file effort, that provided recommendations and best practices for the FBI to follow in its IT processes, including its contracting process. In addition, in our audits we are assessing in detail whether the

FBI applied the lessons learned from other IT projects to its Sentinel procurement.

At this time, we have not found anything to lead us to believe that the time schedule for development of Sentinel is unreasonable. However we are evaluating this issue in our current audit and will continue to evaluate this issue in forthcoming reviews.

Questions for the Record, Senate Judiciary Committee
FBI Oversight Hearing, May 2, 2006

Submitted by Senator Charles Grassley
To DOJ/IG Glenn Fine

1. When did the FBI first receive a copy of your draft report regarding the allegations by former ICE/SAC Houston Joseph Webber of coordination problems between the FBI and ICE on a terrorism financing case?

The FBI received a copy of the draft report on January 27, 2006, for a review of whether it was appropriately classified.

2. How long did the FBI have a copy before a copy was provided to ICE?

After the FBI had reviewed the classification of each paragraph, the report was provided to ICE. ICE received a copy of the draft report, with the FBI's classification markings, on February 17, 2006. Both the FBI and ICE were then asked to provide comments on factual accuracy.

3. Why did ICE not receive a copy of the report for classification or sensitivity review at the same time the FBI received it?

ICE did not receive a copy of the draft report for a classification review at the same time the FBI did because most of the classified and sensitive information in the report originated with the FBI. For that reason, we believed the FBI should review the report for classification purposes before we provided the document to multiple individuals in ICE and elsewhere in government for their review.

ICE has recently confirmed the practicality of this approach. The DOJ OIG and the DHS OIG are now working with the FBI and ICE to produce an unclassified version of the report. The OIGs offered to have the FBI and ICE simultaneously review the final report to provide a line-by-line analysis of whether any material in the report is classified or too sensitive for public release. However, ICE responded that the FBI should review the final report first and provide its classification/sensitivity markings to ICE, and then ICE would review it. ICE reasoned that since most of the classified/sensitive information in the report originated with the FBI, this would be a more efficient way to proceed. The OIGs agreed to the process that ICE suggested.

4. The chapter on the Zacharias Moussaoui case in your report on the FBI's handling of intelligence information before 9/11 has not yet been released. Now that Moussaoui has been sentenced, when do you anticipate releasing a declassified version of that chapter so that the American public can understand better what happened? What action, if any, is required on the part of the FBI before that release can occur?

We currently are in the process of producing an unclassified report for public release. We hope to complete this project by the third week in June. The actions required for the unclassified report to be released are for the OIG to produce what we believe is an unclassified version of the report and then ask the FBI and other intelligence agencies whose information is contained in the report to review the draft. That process is ongoing.

Question for Inspector General Fine
from Senator Charles E. Schumer

When the President signed the PATRIOT Reauthorization Act on March 6, 2006, he issued a signing statement that implied he did not intend to follow the Act's provision that the results of the IG audits mandated by the Act to Congress is required. Do you intend to provide the results of your audits under the PATRIOT Reauthorization Act to Congress as required by that law?

Yes.

Questions for John Gannon

1. Q. Why do you propose putting domestic intelligence under DHS, a department that has consistently failed to live up to expectations?

A. I do not advocate putting domestic intelligence under DHS as presently constituted. It would take a major upgrading and refocusing of DHS consistent with the provisions of the Homeland Security Act of 2002. As such, I believe that a reconstituted DHS would be better positioned than FBI to serve as the focal point for domestic intelligence in the information age. DHS has an organization with mandated outreach to the Intelligence Community, to other USG agencies, to the national laboratories, to state and local governments, to academia, to the private sector, and to foreign counterparts—all of which are key contributors to today's complex domestic threat assessment. I did not rule out this role for FBI, but stressed that the Bureau is way short of doing that job today. These recommended options, moreover, were not the core of my testimony. I argued that America does not have a domestic intelligence capability in the fifth year since 9/11, that this is unacceptable, that the threat to the homeland is global and requires a domestic intelligence capability that is info-tech smart and collaborative across agencies, and that is capable of authoritative strategic analysis and collection against terrorism and other threats to the homeland. My statement to the committee provides an evaluation of the steps we have taken since 9/11, and makes explicit recommendations related to domestic intelligence and intelligence reform in general. We have a pressing need to clarify roles among lead agencies involved with intelligence, including the FBI. I document DHS's shortcomings, as I have observed them first hand, but I attribute these failures to lack of investment by the Executive Branch and acquiescence by Congressional overseers in the failure to implement their own legislation. In this sense, my statement is less an encomium to a DHS that might have been than a respectful criticism of Congressional oversight as it is today.

2. Much of your testimony concerns your plan to push the DHS into the lead role and to relegate the FBI to a minor player in intelligence. However, as you concede, this kind of reform is not likely to pass the Congress. Is there more advice you can give us concerning how we can improve the FBI, if the FBI continues to maintain its status?

A. Most of my testimony relates to an analysis-- which members can accept or not-- of the unprecedented global challenge we face today in domestic intelligence, of our unsatisfactory record thus far in meeting it, of the shortcomings of FBI, and of comprehensive recommendations to do better. This is what I am "pushing," if anything. My discussion of DHS does not fill even three pages of the 15-page, single-spaced statement I provided to the committee. As I suggested in my testimony, the Bureau could undertake this mission if it takes much bolder steps than it has done so far to change its agent-dominated structure, empower intelligence, and alter management rewards and incentives to get itself into compliance with the Intelligence Reform and Terrorism Prevention Act of 2004. This cannot happen without rigorous oversight from the Executive and Legislative branches. I offered personal observations from my career at CIA, briefly in the White House, and most recently on the Hill as to why this mission is so hard for the Bureau to fill and as to why I think we should reconsider the national intelligence mandate we have placed on it. My view is more critical of the Administration and the Congress that it is of the Bureau. I believe that, in the heavy focus on intelligence, we fail to appreciate the growing challenges associated with FBI's traditional law enforcement mission and the difficulty the new intelligence mandate presents for Special Agents in Charge.

3. In your testimony, you say that since 9/11, "Congress has consistently favored creating new 'boxes' rather than fixing or eliminating the old ones—without seriously assessing the cost to existing critical programs." Based on this, if we choose to follow your advice on emphasizing the DHS and de-emphasizing the FBI, what are the costs to the FBI and other intelligence agencies?

A. Minimal costs and perhaps some gains. The FBI would continue to develop an intelligence collection and analytic capability in support of its premier criminal-investigation mission and its evolving counterterrorism capability. It would remain the only Federal agency "running agents" within the United States. Its frustration with the national intelligence mission would be lessened and it would be freed up to improve law-enforcement capabilities that are its strong suit. I believe that the FBI's struggle with its intelligence mission is recognized within the IC, and that a scaling down of that mission would be understood. I consider the option of a revitalized DHS because the Department exists, under-resourced, underachieving, and underappreciated. The Administration and Congress created it with broad outreach to sources of intelligence and information related to domestic security. If we let DHS dissolve, we will need another such collaborative model to manage domestic intelligence. If implemented, such a model would challenge the IC to deal with a new evaluator of US intelligence capability and performance. Some in the IC and the Congressional intelligence committees might not like this. I believe it would be a constructive development.

3. In your testimony, you mention that the Defense Department is "the IC's thousand pound gorilla." Other commentators have similarly complained about the DOD's power, especially over the budget. What would you recommend that we do to make sure the DHS, or the FBI, is not overwhelmed by the DOD?

A. Intelligence reform represents the most significant shift of power in the Federal Government in my career, and perhaps since the National Security Act was passed in 1947. The DNI is a major actor but others have significant power, including the SECDEF, the Attorney General, and the Secretary of Homeland Security. My testimony explains why I believe that DoD, bureaucratically, is now the principal beneficiary of intelligence community reform. Our military is extraordinarily capable, is well funded, and has no match in the Federal Government for smart training and planning, and for exercising its plans. Since 9/11, however, we have seen an alarming failure to develop essential civil capabilities in homeland security and a slow pace of intelligence reform under the DNI. The core problem is that there is minimal Executive Branch supervision of Intelligence Community transformation and inadequate Congressional oversight. I argue that the President needs to exert more control over these principals as they implement his agenda for intelligence reform, including on domestic intelligence. Similarly, the Congressional committees of jurisdiction need to find ways to work together to guide this reform. In an "unregulated market," DoD will continue to gain and, at the other end of the Federal spectrum, DHS will keep on losing.

4. You state in your written testimony that the FBI is not an effective domestic intelligence agency. Yet we have gone five years without another attack by al Qaeda. If the FBI hasn't been effective at preventing further attacks, who has been responsible? Is it solely the work of the DOD and CIA? It doesn't seem to be the work of the DHS?

A. In my statement, I cite three reasons why I believe we have not had another terrorist attack on the homeland since 9/11, and I give credit to FBI for its part. First, the President's bold offense against terrorists anywhere in the world we could find them—engaging our intelligence services as well as our military--has had a major deterrent effect. Second, government efforts at all levels—however uncoordinated and short of our hopes-- to prevent attacks, to secure our infrastructure, and to enhance our response capabilities have raised the cost of doing business here for international terrorists. Processes and procedures at our borders, airports, and ports have improved. Our Coast Guard has never performed better. I would say the same for the United States Secret Service. These are just two of the 22 agencies now incorporated into DHS. At no point did I suggest that FBI was not a contributor to securing the homeland. Neither would I contend, as this question to me does, that DHS has not been an important player in the broad counterterrorism effort. It has. The third factor I point to is the bedrock democratic nature of our society, in which civil liberties are enshrined and the right to criticize government is not only allowed but protected under the Constitution and celebrated in practice. As a people, we are not afraid to express our grievances openly or to assail our Federal, state, or local leaders. Paradoxically, however, an underlying trust of government exists in our society side by side with a militant distrust of government. We can expect that international terrorists will try to enter our country and to operate here, as the 9/11 hijackers did. But I would argue that they are likely to find limited ground to breed terrorism in America, and they are more likely to find people ready to cooperate with Federal, state, and local law enforcement against them. Paradoxically, our freedoms make us vulnerable to attack but also protect us from it. For these "civil liberties" reasons in part, I endorse a collaborative model for domestic intelligence and oppose the establishment of a new centralized domestic intelligence service under the Executive Branch.

5. The FBI leadership has worked diligently for five years to overturn an institutional bias from the reactive chasing of criminals to a proactive prevention of terrorism. From all measurable appearances, this change is taking place. Why do you suggest undoing that change instead of allowing it to continue? Shouldn't we expect it to take some time?

A. *I do not accept the premise of this question, nor the suggestion that I propose "undoing" positive change in the Bureau. The WMD Commission, which submitted its report just over a year ago, painted a starkly different picture from "all measurable appearances." On the Bureau's new Directorate of Intelligence, it stated in Chapter 10 that "We concluded that the directorate's lack of authority was pervasive. We asked whether the Directorate of Intelligence can ensure that intelligence collection priorities are met. It cannot. We asked whether the directorate directly supervised most of the Bureau's analysts. It does not. We asked whether the head of the directorate has authority to promote—or even provide personnel evaluations for—the heads of the Bureau's main intelligence-collecting arms. Again, the answer was no. Does it control budget or resources of units that do the Bureau's collection? No. The DNI's appointment influence over the head of the directorate therefore does little to bring the FBI's national security activities into a fully functioning Intelligence Community." Again, the commission said this just over a year ago, not five years ago. As you know, the President accepted the commission's report and recommendations to consolidate the Directorate of Intelligence, the Counterterrorism Division, and the Counterintelligence Divisions. While I am more skeptical than my questioner, I concede that the committee is in a much better position than I am to evaluate progress since the establishment of the National Security Branch. As to the final question, I believe we have taken way too much time to get where we are given the gravity of the 9/11 attack and what it told us about our shortcomings in domestic intelligence.*

6. How do you square your criticism of the FBI on its failure to provide "authoritative analysis" on the domestic threat when NCTC is, by law, the focal point for such analyses?

A. This goes to the core of my effort to define domestic intelligence in the context of globalization—which the committee if free to reject as I now assume it has. For my part, I do not accept the premise of your question. The Intelligence Reform and Terrorism Prevention Act of 2004, Title I, section 119 (d) (1) states that the NCTC shall serve "as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United Sates Government pertaining to terrorism or counterterrorism excepting intelligence pertaining to domestic terrorists and domestic counterterrorism." So here the law excludes from NCTC responsibilities "domestic terrorists and domestic counterterrorism" by a narrow definition that I believe does not apply to today's interconnected world. The threat to the homeland is largely from abroad and this means that our analysis of it must be "borderless." Later on, Title II, section 2002 (2) (6) gives the FBI responsibility for "Strategic Analysis," a job that I know the Bureau is taking seriously. But strategic analysis of what? Domestic militias? The FBI is forced by the targets it faces to integrate foreign and domestic intelligence in its own strategic analysis. As I see it, the NCTC is the "primary" but not exclusive analyst, the "net assessor" of the threat to the homeland , but this does not relieve the FBI of its own responsibility to analyze the terrorist threat. Your question, in my judgment, is symptomatic of the Congressional tendency to "pack it in neat boxes."

7. What is your concept for how Field Intelligence Groups operate? Have you visited one?

The Field Intelligence Groups, which were established late in 2003 in the Bureau's fifty-six field offices, consist of all-source analysts, linguists, special agents, and reports officers. I believe our CODEL met with the FIG in Los Angeles some time in late 2004 or 2005. The FIG, as I understand it, is intended to integrate and "synergize" intelligence and law enforcement operations in the field, to strengthen the role of analysts in guiding this process and in managing production—especially strategic analysis. My testimony commends this initiative and credits it with improving intelligence support to the Bureau's increasingly complex criminal-investigation mission. I claim no first-hand knowledge of this program today. I question, however, whether it can succeed over the long term unless the analysts are part of a distinct career service within a Directorate of Intelligence that has control of its own budget and personnel, and has a direct line to the FBI Director—independent of agents. I note that the WMD Commission last year suggested that the FIGs thus far tended toward case-related tactical—not strategic--work. I would guess that the program is uneven in quality from place to place and is still nascent over all. .

8. When was your last FBI field visit?

I will ponder on my own time the point of this question. As I state in the second paragraph of my written statement, I have not had official contact with the Bureau since I left the Hill for the private sector in February 2005. I have, however, had several conversations over the past year with active FBI personnel, including senior officers. I last met with a Special-Agent-in Charge on 20 September 2005, when I visited Trenton, New Jersey, to address the Third Annual Counter-terrorism Conference sponsored by New Jersey's Office of Counterterrorism.

As the team leader for intelligence on the Transition Planning Office (TPO) for the Department of Homeland Security from 2002-2003, and as Staff Director of the House Select Committee on Homeland

Security from 2003-2005, I had frequent contact with the Bureau. I had an FBI detailee on the TPO and Bureau liaison to the Select Committee. From 2002 to 2005, I made official visits to Boston, Houston, Los Angeles, Seattle, Detroit, and Washington, D.C. (FBI headquarters and the National JTTF). I met with Bureau personnel at most of these locations.

9. Like the CIA\Directorate of Intelligence\, the FBI has its own Directorate of Intelligence, with independent oversight of FBI analysts. How does that structure differ from the model you ask for?

The Directorate of Intelligence (DI) at CIA, which I led, and of the Directorate of Intelligence at FBI, are strikingly different models. The CIA's DI is largely a Washington-based community of regional and functional subject-matter experts. It is a hub-and-spoke design in which analysts are detailed to other directorates, different agencies, and overseas stations but they are evaluated and promoted—or not--by the DI career service, even when detailed elsewhere. The DI hires, trains, manages, and deploys its analysts—independent of the operations directorate. The Deputy Director for Intelligence, who leads the DI, controls his/her budget and personnel. The separate analytic structure, with a direct line to the CIA Director, protects analysts whose work, at times, may challenge the views of Agency operations officers and top managers, as well as policymakers.

The FBI, as I have observed it, has a more decentralized model which has some analysts at headquarters but deploys most of them to Field Intelligence Groups. You state that the FBI Directorate of Intelligence has "independent oversight" over all these analysts. I doubt that this is in any way comparable to the authority of the CIA's DDI. The WMD Commission last year found (Chapter 10) that: "the Directorate of Intelligence itself has no authority to direct any of the Bureau's intelligence investigations, operations, or collections. It currently performs no analysis, commands no operational resources, and has little control over the 56 Field Intelligence Groups, which according to the FBI, 'manage and direct all field intelligence operations.' " The report asserts that the Executive Assistant Director in charge "lacks direct supervisory authority over the vast majority of the FBI's analysts." In short, the Bureau is attempting to grow an analytic capability out of a criminal-investigation organization, not structuring it independently. If the Committee is satisfied that the situation has changed dramatically since the adoption of the Commission's recommendation to form the National Security Branch, then so be it. I would be pleased if such were the case. The DNI should now know the objective reality inside the Bureau.

The domestic intelligence model I describe would borrow from the CIA example, but it would have to be built on a foundation of unprecedented interagency collaboration to incorporate state and local governments and to access the broad sources of information and intelligence needed to meet the challenge. A reconstituted DHS, or a successor, could be the hub of a decentralized national network for domestic intelligence with state-of-the-art, multi-level-security communications, not a centralized intelligence service under the executive branch.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 30, 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 May 2, 2006. The subject of the Committee's hearing was "Oversight of the Federal Bureau of Investigation." The FBI submitted these responses for clearance on July 10, 2006. We hope this information is helpful to the Committee.

The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to the submission of these responses. 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,

James H. Clinger

James H. Clinger
Acting Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Responses of the Federal Bureau of Investigation Based Upon the May 2, 2006 Hearing Before the Senate Committee on the Judiciary Regarding FBI Oversight

Questions Posed by Senator Specter

FBI Classified Information Questions

1. What is the FBI doing to prevent leaks of classified information from within its own ranks?

Response:

All new FBI employees receive briefings on the importance of protecting classified information, the protocols of addressing FBI issues with external contacts, and administrative measures which the Bureau takes against those who mishandle classified material. In addition, new employees sign a Classified Information Non-Disclosure Agreement before they come in contact with any classified information. For employees who are already on board, the FBI also presents security awareness training and mandatory information security training on a regular basis.

Throughout employment with the FBI, all employees undergoes a Periodic Reinvestigation every five years which may include a Personnel Security Polygraph (PSP) examination. The PSP focuses on counterintelligence issues, to include unauthorized disclosures. The PSP is used not only to identify any potential unauthorized disclosures of classified information that may have occurred, but also to serve as a deterrent to unauthorized disclosures by FBI personnel.

2. On April 30, 2006, The New York Times reported that the Bush Administration is attempting to prosecute publication of classified information by reporters under the Espionage Act of 1917, citing justification given in Justice White's dissenting opinion of *U.S. v. New York Times* (the Pentagon Papers case). Given the FBI's recent attempt to seize Jack Anderson's papers, does the FBI agree that reporters are vulnerable to prosecution under this act?

Response:

Please refer to the 6/6/06 testimony before this Committee of Matthew W. Friedrich, Chief of Staff and Principal Deputy Assistant Attorney General of the

Department of Justice (DOJ) Criminal Division, regarding the application of the Espionage Act of 1917 to the prosecution of reporters.

3. The FBI has stated that under the law, no private person may possess classified documents that were illegally provided to them by unidentified sources, and that such classified documents remain the property of the US government? Specifically, under which law?

Response:

Numerous mechanisms are available to protect the government's property interest and right to possess and control the dissemination of classified information. Pursuant to 18 U.S.C. § 793, whoever is in unauthorized possession of documents or information related to the national defense and willfully retains the same, and fails to deliver this material to the officer or employee of the United States entitled to receive it, is subject to imprisonment and fine. In addition, 18 U.S.C. § 3663(b)(1) provides that, when sentencing a defendant convicted of a Title 18 offense, the court may order restitution, including the return of stolen property. Executive Order 12958, as amended, establishes that information remains classified and must be protected from unauthorized disclosure until it is officially declassified. This Executive Order further requires that classified information remain under the control of the originating agency and specifies storage and distribution restrictions. Under common law, the owners of stolen property generally retain ownership of the property, even if it is passed to a innocent third party.

4. Do you agree with the 1971 Supreme Court decision in *U.S. v. New York Times* in which the court stated that a newspaper could be "vulnerable to prosecution"?

Response:

Please see the response to Question 2, above.

5. A recent *New York Times* article (Liptak, 04/30/06) reported that the FBI recently made efforts to reclaim classified documents allegedly in the personal files of the late columnist Jack Anderson. The FBI has stated no private person may possess classified documents that were illegally provided to them by unidentified sources, and that such classified documents remain the property of the United States government. The *Times* article refers to two Federal statutes in the Espionage Act which prohibits: (1) anyone with unauthorized access to documents or information concerning the national defense from telling others (18 U.S.C. § 793); and (2) the publication of government codes and other "communication intelligence activities" (18 U.S.C. § 798). What is your interpretation of these statutes as they relate to the issue at hand? What is your interpretation of the

following statutes, which might also be relevant to the issue at hand: 50 U.S.C. § 421; 42 U.S.C. § 2277; 50 U.S.C. § 783?

Response:

This question requests a legal opinion concerning the interpretation of the specified statutes. The FBI defers to DOJ's longstanding policy of declining to render legal opinions to Congress (except comments on proposed legislation) and others outside the Executive Branch. *See* Request of the Senate for an Opinion, 39 Op. Att'y Gen. 343, 344, 347 (1939).

6. In your opinion, did Congress intend 18 USC § 798 and 50 USC § 421 to apply to the dissemination of classified information to newspapers and reporters? How about the other statutes mentioned above?

Response:

The referenced statutory provisions identify the classes of persons and the conduct to which they apply. The FBI is not aware of any class of persons, covered by a particular statutory provision, that is generally immune from prosecution under that provision.

7. How have these three statutes been applied in the past? Who has been prosecuted under these statutes?

Response:

Computerized FBI statistical accomplishment records do not reflect prosecutions occurring under 50 U.S.C. § 421 or 42 U.S.C. § 2277. Two subjects were charged under 50 U.S.C. § 783. Thomas Joseph Dolce, a weapons analyst at the Aberdeen Proving Ground in Maryland, pled guilty to passing classified defense information to the South African government and was sentenced in Federal Court on 04/19/89 to 10 years' incarceration and fined $5,000. Douglas Simon Tsou, an FBI Language Specialist in the Houston Division, was convicted of passing classified defense information to representatives of the government of Taiwan and sentenced on 01/22/1992 to 10 years in federal prison. Sharon M. Scranage pled guilty to violation of 50 U.S.C. § 421 in 1985 and was sentenced to 5 years' imprisonment, which was ultimately reduced to two years. Lawrence Anthony Franklin pled guilty in January 2006 to violations of 18 U.S.C. §§ 793 and 371 (conspiracy to violate 50 U.S.C. § 783) and was sentenced to 12.5 years in prison. Frederick C. Hamilton pled guilty in 1993 to two counts under 50 U.S.C. § 783(b) and was sentenced to 3 years and one month of imprisonment.

8. Under which statute do you seek to reclaim the Jack Anderson documents?

Response:

The FBI met with the Anderson family in an effort to review the files with their consent. At this time the FBI is not seeking to reclaim any documents.

9. In your testimony, you note that it is imperative to protect the nation's security while still preserving our civil liberties. Do you agree that prosecuting reporters under the Espionage Act would protect the nation without unduly burdening freedom of the press?

Response:

DOJ has never in its history prosecuted a member of the press under Section 793, 798, or any other section of the Espionage Act of 1917 for the publication of classified information, even while recognizing that such a prosecution is possible under the law. DOJ's policy in this regard is published at 28 C.F.R. § 50.10, which requires that the Attorney General approve not only prosecutions of members of the press but also investigative steps aimed at the press, even in cases where the press is not itself the target of the investigation. This policy - voluntarily adopted by DOJ - ensures that any decision to initiate criminal proceedings against the press is made at the very highest Departmental level and only after all relevant facts and circumstances have been considered and other options have been exhausted. The Attorney General has stated that DOJ's "primary focus" is on the leakers of classified information, as opposed to the press, and that the country's national security interests and First Amendment interests are not mutually exclusive and can both be accommodated. The FBI fully acknowledges that freedom of the press is vital to our nation and protected by the First Amendment to the Constitution.

10. What papers is the FBI attempting to seize from Jack Anderson, and why is it trying to take them? Considering that Anderson stopped writing his column in the mid-1980's, at best these papers are twenty years old, and they should have little to do with current issues. There have been allegations that the FBI is interested in them because Anderson discovered certain things about J. Edgar Hoover's personal life; is this true? Or do these papers concern the recent court case against two former AIPAC lobbyists, Steven J. Rosen and Keith Weissman? Feel free to answer this question in a classified session, if you so wish.

Response:

The FBI contacted the Anderson family to seek their consent for an FBI review of files in their possession. Through discussions with the family and others, the FBI confirmed that the files contained documents marked as classified and that the

papers were being reviewed for purposes of making them publicly available. Consistent with our obligations under existing law and Executive Orders, we sought to review the papers to determine, among other things, whether public disclosure of any of them would cause a risk to national security. Access was not sought because Anderson allegedly had information regarding former Director Hoover's personal life.

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

FBI TRILOGY Questions

11. At least $7.6 million worth of equipment purchased for Trilogy is unaccounted for in a GAO report entitled "Weak Controls over Trilogy Project Led to Payment of Questionable Contractor Costs and Missing Assets" from February 2006. What steps have been taken to locate these assets? Are the Trilogy contractors required to reimburse the FBI for equipment losses? What is being done to ensure that the same missteps are not repeated during the Sentinel or subsequent purchasing projects?

Response:

To provide context for the Report's findings regarding property controls, the FBI notes that more than 44,000 pieces of accountable property were successfully deployed and tracked in the FBI's property management system during Trilogy's development. The Government Accountability Office (GAO) report initially identified 1,404 items (approximately 3% of the total) of unaccounted for or improperly documented property. As of April 2006, the FBI had accounted for more than 1,200 of these items, and we are continuing our efforts to locate or document the remaining Trilogy assets.

It was always the intent of both the FBI and the General Services Administration's (GSA) Federal Systems Integration and Management (FEDSIM) Center to have the Defense Contract Audit Agency (DCAA) conduct final close-out audits to assess final costs, including direct and indirect labor costs. This is the appropriate means of identifying and addressing any potential overpayments to contractors. Close-out audits are designed to disclose and resolve questionable costs of the type GAO reported, as well as costs deemed unallowable under the contract. The initiation of the close-out audits has been delayed until final rates for both the prime contractors and all subcontractors have been approved by DCAA and final reconciliation is completed by both prime contractors. At that time both prime contractors will be able to submit their final invoices and DCAA will be able to complete the final closeout audit. While the prime contractors are reconciling their subcontractor costs and waiting for DCAA approval of their final rates,

GSA/FEDSIM is finalizing negotiations with the GSA Deputy Assistant Inspector General (IG) for Auditing, FBI, and DCAA to have DCAA conduct an overall program audit of both task orders. The scope of the program audit will include the costs identified by GAO as potentially questionable. Upon completion of the program audit, DCAA will conduct the final closeout audit of both task orders. GSA and the FBI will monitor the progress of the close-out audits and will ensure all areas of concern cited in the Report, including the direct labor rates charged by the contractors and their subcontractors, are thoroughly reviewed and resolved.

In preparing for Sentinel, the FBI has taken care to lay the groundwork for a successful major investment. We have created a strong program management office (PMO) with clear reporting lines to the Chief Information Officer (CIO) and the FBI Director. We have staffed the PMO's Office with highly skilled technical, programmatic, business management, and administrative subject matter experts. The FBI will augment that staff with audit support from the FBI's Finance Division to review invoicing, as well as an independent verification and validation (IV&V) contractor to review the accuracy of the development contractor and the PMO, ensuring proper execution and delivery of the Sentinel system.

The GAO and Department of Justice (DOJ) IG are both performing audits of the Sentinel program throughout its development to provide assessments concerning the PMO's progress in delivering and implementing the Sentinel system. The DOJ CIO, Deputy Attorney General (DAG), Office of the Director of National Intelligence (ODNI), and Office of Management and Budget (OMB) are all meeting with the Sentinel Program Manager and senior managers in the Office of the CIO (OCIO) and the Finance Division in various forums to ensure the Sentinel program is proceeding as planned and the contracted system will be delivered to the users on time, within cost, and with the required capabilities.

In accordance with the FBI's Life Cycle Management Directive (LCMD), the Sentinel program is required to present its programmatic, architectural, technical implementation, and operational readiness updates to several enterprise level control boards in order to ensure the end product of the development activity meets the criteria for investment alignment with the FBI's strategic planning, enterprise architecture, systems engineering standards, and operation and maintenance policies and practices. Finally, the contract vehicle is structured so that the contractor has clear reporting requirements, deliverables, and milestones.

12. GAO reports over 1200 pieces of equipment, worth $7.6 million, is unaccounted for from the Trilogy project. Additionally, 30 pieces of equipment worth almost $167,000 were reported as being lost or stolen. Does it concern you that assets that may be sensitive in

nature are not only missing from FBI warehouses but may also have been stolen? Can you describe the protocols the FBI uses to track its assets?

Response:

Any loss or theft of property is a concern, and the FBI took immediate action to locate those items listed as unaccounted by the Report that, if lost, would have posed a potential security breach.

The FBI tracks assets, from acquisition through disposal, consistent with the Federal Management Regulation (41 C.F.R. § 102), the DOJ Property Management Regulations (41 C.F.R. § 128), and applicable Federal property management regulations promulgated by GSA and OMB. This includes maintaining inventory, upon receipt, for all accountable property in the system of record. Accountable property includes all hardware with an acquisition cost of $1,000 and greater, all software with an acquisition cost of $500,000 and greater, and - regardless of cost - all firearms, COMSEC equipment, laptop computers, jewelry, and central processing units. These five classes of property are considered controlled personal property, or sensitive property, which are subject to a high probability of theft or misuse due to their inherent attractiveness and/or portability. Property valued at $25,000 or more is a capital asset. Property management is decentralized in the FBI, with accountability assigned to an Accountable Property Officer in each Division, Field Office, or Legal Attaché. The Finance Division exercises centralized oversight of property management through annual inventory of capital assets and sensitive property, biannual inventory of all accountable property, semi-annual reviews of orders and transfers, and periodic reviews and audits of sensitive and accountable property.

The agreement with the Trilogy contractor resulted in modified property management procedures. In its discussion of control over Trilogy assets, the Report notes the FBI did not require compliance with its normal procedures for documentation of shipments from contractors. In discussions with GAO staff and in materials provided to GAO, the FBI explained that the normal policy was modified in order to maintain the contractor's control of the shipments until the contractor completed the installation process. In effect, while the FBI received the shipments, we did not accept delivery until the contractor processed the contents of those shipments. This modification for the Trilogy program should not be construed as a systemic lapse in the FBI's property management policies.

The FBI is focused on improving property management, reinforcing existing policies and instituting stronger reporting and accountability across the FBI. KPMG, the independent auditor cited in the Report and contracted by the DOJ IG to check the health and accuracy of the FBI's financial statements, recently

changed the FBI's property and equipment grade from a material weakness to a reportable condition, stating, "During fiscal year 2005, the FBI showed progress in resolving several of the issues noted in prior year audits, and has worked towards implementing effective and routine controls."

FBI Sentinel Questions

13. A *U.S. News and World Report* article entitled "High tech's High Stakes at the FBI" (U.S. News & World Report, 4/17/06), states "Some executives believe the bureau's computer upgrades (i.e. Sentinel) could ultimately total a billion dollars--double the projected costs ... at the bureau, tensions are rising as many officials stew over what they view as imprudent across-the-board cost cutting to hide Sentinel's *real* price tag from Congress and spare Mueller further ignominy." Including the costs of transferable assets from VCF, what is the total cost of Sentinel?

Response:

The total value of the contract with Lockheed Martin is $305 million over 6 years, including both development and Operations and Maintenance (O&M). The FBI estimates that the total cost of the Sentinel Program, including program management, systems development, O&M, and IV&V, will be $425 million over 6 years. Sentinel's total cost is depicted in the below tables. (The first table breaks the costs out by activity, while the second table depicts costs by phase.) The assets developed in the course of the Trilogy project, including Virtual Case File (VCF), were reinvested in the FBI's overall enterprise network before award of the Sentinel contract and are, therefore, not appropriately attributable to Sentinel.

ACTIVITY	COST
Pre-Award	$ 4.3M
Program Management Operations	74.8M
IV&V	6.0M
Risk Management	35.0M
Development Contract	232.4M
Operations and Maintenance	72.7M
TOTAL	**$425.2M**

PHASE	COST
Pre-Award	$ 4.34M
Phase 1	97.0M
Phase 2 (+Pre-FOC O&M)	150.3M
Phase 3 (+Pre-FOC O&M)	51.7M
Phase 4 (+Pre-FOC O&M)	79.8M
O&M Years 1 and 2	42.1M
TOTAL	**$ 425.24M**

14. At our last FBI Oversight hearing in July 2005, we discussed the timing of completion of the Sentinel project and how that might impair the effective coordination of intelligence efforts against current terrorist threats. Now that you have more concrete plans as to when Sentinel will be completed, do you anticipate this being a problem?

Response:

No, we do not anticipate this being a problem. With the development of both the Case Management Line of Business and the National Information Exchange Model (NIEM) to improve intelligence efforts, the timing of the Sentinel project is good, since the Sentinel efforts can assist in guiding both.

FBI Translation Problems Questions

15. In your written responses from last July's hearing, over 3,000 employees and contractors are reported to be certified in language proficiency at or above the working proficiency level. What is the turnover rate among these employees and contractors?

Response:

For the past 5 years, annual language analyst attrition has ranged between 5 and 8%, and contract linguist attrition has been between 9 and 11%. Competition for high-quality language services in the public and private sectors is fierce, and others are willing to pay steep premiums for resources already vetted by the FBI. Many departing employees have cited the lure of the higher salaries offered in the private sector as the primary reason for their separation. Despite these factors, however, Foreign Language Program attrition remains relatively low. Innovative retention programs, such as a Foreign Language Proficiency Pay Program, are currently under consideration within the FBI. These programs, partnered with other career-enhancing opportunities now being afforded to linguists, are expected to reduce attrition even further.

16. According to IG Glenn Fine, the FBI's counterterrorism audio backlog was 4,086 hours as of April 2004 and in a follow up review, has doubled to 8,354 hours. What is the current amount of unheard audio? What have you done to remedy this problem?

Response:

Of the several hundred thousand hours of audio materials and almost two million pages of text collected in connection with counterterrorism investigations over the last 4 years, only 1.35% of all audio (7,028 hours out of 519,217 hours collected), 0.48% of all electronic data files (26,518 files out of 5,508,217 files collected), and less than 0.0001% of all text (62 pages out of 1,847,497 pages collected) were backlogged as of February 2006.

Of the accrued backlog, 31.23% is attributable to elongated "white noise" microphone recordings resulting from certain techniques not expected to yield intelligence of tactically high value (2,195 hours of open microphone recording out of the total audio backlog of 7,028 hours). Another 46.1% (3,240 hours out of the total audio backlog of 7,028 hours) is audio from very obscure languages and dialects. The FBI is currently recruiting the linguists necessary to address this backlog.

The FBI now possesses sufficient translation capability to promptly address all of the highest priority counterterrorism intelligence, often within 24 hours. The FBI's prioritization and triage processes are helping to reduce the accrued backlog. The FBI continues to hire as many linguists as can be cleared, and we are hiring them in field offices where traditionally there were none. The FBI currently has 1,379 linguists, with the capability of translating in approximately 100 languages, a 76% increase in the overall number of linguists since 9/11/01, with the number of linguists in certain high priority languages (e.g., Middle Eastern and North African languages) increasing by 200% and more. In addition, the FBI is obtaining qualified and cleared linguist support from other available sources (including from within the United States Intelligence Community (IC)) through the National Virtual Translation Center, as well as from the language programs of allied intelligence agencies.

17. According to FBI statistics, it takes approximately 13 to 14 months to hire a contract linguist. Has improvement been made in this area?

Response:

During the past 18 months, the FBI has worked to implement re-engineered procedures that will increase the efficiency of the processing lifecycle of contract linguist applicants. Through a contractor-based partnership, the FBI is designing

an applicant communication and management system, called the Contract Linguist Automated Support System (CLASS), for all contract linguist applicants.

This initiative was based on a business process improvement study, the purpose of which was to identify, document, and provide solutions for bottlenecks, inefficiencies, outdated technologies, and underlying environmental and cultural factors that contribute to the lengthy contract linguist applicant process. The study generated recommendations that will enhance many of the processing steps, including prescreening, language proficiency testing, suitability determinations, contract issuance, and invoice payments.

The contractor has gathered nearly all the information necessary for the design and development of CLASS. The FBI's robust LCMD ensures this system will meet the criteria established by our Records Management, Information Technology (IT) Operations, and Security Divisions, as well as by the FBI's Office of the General Counsel (OGC). With an anticipated rollout in the summer of 2007, CLASS is expected to reduce contract linguist application cycles by as much as five months.

18. It has been alleged in an article that despite a shortage of Arabic translators, the FBI turned down applications for linguist jobs from nearly 100 Arabic-speaking Jews in New York following the World Trade Center attacks. (Sperry, 10/09/03) Is this true? It has further been alleged that "the FBI was concerned that many of the applicants were "too close to Israel," and might lack the objectivity to accurately translate the Arabic recordings and writings of Muslim terrorist suspects under investigation. Indeed, some worked for the Israeli military." Why were all of these individuals turned down? Are non-Jewish Arabs similarly evaluated as to potential biases?

Response:

These unsubstantiated allegations relate to a meeting between our New York Field Office (NYFO) and Sephardic Bikur Holim (SBH), a New York-based charity, after 9/11/01 to discuss how the charity's membership could assist the FBI. During this meeting, NYFO representatives explained that generally only United States citizens can be considered for the FBI's contract linguist positions because of the requirement for a "Top Secret" security clearance. Executive Order (EO) 12968, "Access to Classified Information," Section 3.1(B), provides that, with certain limited exceptions, "access to classified information shall be granted only to employees who are United States citizens." (While the EO does permit an agency to grant limited access to foreign nationals under some circumstances, both the scope of the work required and the restrictions placed on that access militated against the exercise of that authority in this case.)

After this meeting, an SBH representative provided NYFO with the names and telephone numbers of possible candidates and NYFO personnel immediately contacted them. Because many of these individuals reported that they were not United States citizens, we did not invite them to apply for contract linguist positions. However, we did encourage individuals who were United States citizens to submit applications.

The SBH list included 55 type-written names and 4 illegible handwritten names. Of the 55, 32 did not apply for positions, 3 submitted applications but were discontinued because we were unable to contact them using the information provided in their applications, and 2 withdrew from processing before proficiency testing. 18 of the listed individuals submitted to the first phase of the application process: language proficiency testing. Of these:

- 15 applicants were discontinued because they failed to pass language proficiency tests;
- 1 applicant was considered for a language specialist position in 1999, but was discontinued during the course of the background investigation based on a lack of candor;
- 1 applicant passed language proficiency tests but was discontinued because the polygraph examination indicated deception; and
- 1 applicant successfully completed each stage of processing and was approved as a contract linguist in October 2003.

All SBH members who applied for contract linguist positions were processed in a manner fully consistent with FBI rules and procedures. One of these applicants successfully completed the vetting process and is now making a valuable contribution to the FBI as a contract linguist assigned to NYFO. These results are not inconsistent with our normal rate of successful contract linguist applications.

FBI Seaport Security Questions

19. A recent IG report, "FBI's Efforts to Protect the Nations Seaports," indicates that unless agreements are reached for incident command and other coordination issues, the overlapping responsibilities of the Coast Guard and the FBI could result in confusion in the event of a maritime incident. What is the FBI doing to reach these agreements? When will these agreements be finalized?

Response:

The FBI is actively working with the United States Coast Guard (USCG) to resolve coordination issues in advance of actual threats and incidents in the maritime domain. The FBI's efforts are conducted in accordance with the Maritime Operational Threat Response (MOTR) Plan, which was approved by the President and is one of eight supporting plans under the National Strategy for Maritime Security as required by National Security Presidential Directive 41/Homeland Security Presidential Directive (HSPD) 13. The MOTR Plan was developed under the joint leadership of the Department of Homeland Security (DHS) and the Department of Defense (DoD), with DOJ and FBI participation. The current MOTR Plan is an interim plan that was approved by the President in October 2005. This interim plan is currently being revised, and we anticipate that the final plan will be approved by the President by late 2006. The final MOTR Plan will recommend protocols for each agency and will provide guidance for interagency coordination in response to maritime threats and incidents. After the final MOTR Plan is adopted, the FBI and USCG will address the need for an MOU, if any.

The MOTR Plan provides a framework for interagency communication and coordination in response to maritime threats and incidents. MOTR conference calls, made through the existing network of federal command centers, have been used to successfully resolve several real-world incidents over the past few months. The FBI and USCG agree that these coordination mechanisms have dramatically improved the operational response to maritime threats and incidents, and we have jointly briefed the MOTR Plan to interagency audiences.

The FBI has taken several additional steps to ensure a coordinated response to an incident of maritime terrorism. In July 2005, the FBI initiated the Maritime Security Program (MSP), the mission of which is to prevent, disrupt, and defeat criminal acts of terrorism directed against maritime assets and to provide counterterrorism preparedness leadership and assistance to Federal, state, and local agencies responsible for maritime security. The MSP will complement the efforts of other United States Government entities, focusing on core FBI competencies that include the establishment of a human intelligence (HUMINT) base, the collection and distribution of relevant information and intelligence, the preparation of threat and vulnerability analyses, and the provision of investigative support. The MSP emphasizes the importance of its liaison relationships with the USCG and other agencies, participating with the Coast Guard Investigative Service (CGIS) and others in formal and informal interagency working groups. Recently, both the USCG and Naval Criminal Investigative Service (NCIS) have assigned full time representatives to the MSP.

The MSP also provides guidance to approximately 80 Maritime Liaison Agents (MLAs), who are assigned to the FBI's Joint Terrorism Task Forces (JTTFs) throughout the United States. MLAs include FBI Special Agents (SAs) as well as JTTF Officers from the CGIS, NCIS, state and local port authorities and police departments, and others. The FBI recently hosted an MLA training conference that included representatives and presentations from the FBI, DOJ, USCG Headquarters, USCG field operations, CGIS, NCIS, and other Federal and local law enforcement agencies. Conference training included the authorities and capabilities of these agencies as well as best practices and guidelines for operational responses to maritime terrorism threats and incidents.

The FBI and the USCG train together to ensure coordination and interoperability in response to maritime terrorism threats and incidents. Fifteen of the FBI's Special Weapons and Tactics (SWAT) teams are Enhanced Maritime SWAT Teams with specialized training and equipment. These enhanced teams are available to conduct joint exercises with the USCG. In addition, the USCG has invited representatives of the FBI's Hostage Rescue Team and Weapons of Mass Destruction Operations Unit to act as observers and to provide feedback during an upcoming exercise.

20. This same IG report also states that the FBI is concentrating its intelligence efforts on a narrow group of attack scenarios and not devoting resources to high-risk areas. For example, the FBI is concentrating significantly on attacks carried out by combat swimmers and not the smuggling of a weapon of mass destruction being shipped in a cargo container. What is the FBI doing to address this concern?

Response:

The FBI is responsible for acting on maritime threats that may have a nexus to terrorist or criminal acts directed against the United States or its interests and, for this reason, it does not concentrate intelligence efforts solely on a narrow group of attack scenarios. To ensure the FBI is positioned to efficiently and effectively execute its maritime responsibilities, the FBI initiated the MSP, which has the full-time participation of both the NCIS and USCG in order to provide MSP management at the national level. Through the MSP, the FBI, NCIS, and USCG jointly and collaboratively address all identified maritime threats.

21. The FBI has instituted Maritime Liaison Agents (MLA). These agents are assigned to FBI field offices and are responsible for coordinating with the agency's maritime partners including CBP and the USCG. However, the IG audit states that the FBI assigns MLA's indiscriminately, without assessing the threat and risk of terrorists attacking each port. This has led to irrational decisions, such as assigning only one MLA to the New Orleans field office, which has six significant ports in its territory, while assigning five MLA's to the

Louisville field office, which has no strategic ports in its area. Is the FBI preparing to implement a threat assessment plan for the positioning of MLA's? And if not, why not?

Response:

In July 2004, the FBI established a requirement that Field Offices having maritime liaison responsibilities in connection with oceans, rivers, or large lakes identify field personnel to be assigned to the MLA Program as a collateral duty. Other than the requirement to establish the MLA position, how maritime liaison is addressed by each Field Office from a resource standpoint is left to the discretion of the Special Agent in Charge (SAC). For example, the Louisville, Kentucky, Field Office has 11 "resident agencies" dispersed throughout the state. The Louisville SAC determined that maritime liaison activities could best be managed in his Field Office by assigning MLA collateral duty to five SAs stationed in that Division's resident agencies because those SAs are most familiar with the maritime activities and venues and with the Federal, state, and local resources and personnel in their assigned areas. By contrast, the New Orleans Field Office includes a significantly different maritime venue, and that SAC's assessment led to a different approach. In the New Orleans Division, two JTTF officers are assigned as MLAs and have this role as their primary responsibility. In addition, because of the prevalence in southern Louisiana of maritime resources and personnel from the USCG, Customs and Border Protection, and state and local law enforcement agencies, the FBI is able to leverage these resources in the New Orleans Division, which is not necessarily possible in other areas.

22. The FBI does not have a method of tracking the amount of time its agents spend preventing or investigating maritime terrorism. Currently, under the FBI's case classification system, most MLA activities are designated as "Counterterrorism Preparedness - Other." This classification is not specific enough to allow managers of the FBI's maritime efforts to determine the amount of resources the FBI is spending maritime issues, which prevents the implementation of a risk-based counterterrorism program. Is the FBI planning on changing its classification system to solve this problem? If not, why not?

Response:

Because of the establishment of the MSP and the requirement to designate MLAs in all FBI Field Offices, the FBI's focused maritime security work has increased considerably. This increase has demonstrated a need to review our classification system to determine if changes are warranted. This review is ongoing.

Random Questions

23. Several times, the FBI has refused to produce its agents for interviews with the Judiciary Committee. Each time, they have claimed that existing DOJ policy bars them from producing these agents, citing a letter, originally sent out in 2000, written by then Assistant Attorney General Robert Raben. However, the DOJ/FBI's reasoning behind this policy is not a correct reading of the law and/or history. (see CRS Report "Investigative Oversight" by Rosenberg, 1995) Does the FBI support this policy of impeding Congressional oversight? If so, will they be willing to produce more supportive evidence for this policy? If not, are they willing to go on record as opposing this policy?

Response:

The FBI is committed to complying with Congressional oversight requests to the fullest extent consistent with the constitutional and statutory obligations of the Executive Branch and to making every effort to accommodate the needs of the legislative branch to perform its oversight function. We support DOJ's policy of protecting the independent judgment of line SAs by ensuring that the supervisory personnel who serve as decisionmakers are the ones who answer to Congress for those decisions. Please note that the January 27, 2000 letter from Assistant Attorney General Robert Raben cites case law, formal DOJ legal opinions, and correspondence from members of the United States Senate and House of Representatives in support of its policy for responding to Congressional oversight requests.

24. Glenn Fine, the Justice Department's Inspector General, said in a February 17, 2006 briefing that the FBI email system automatically deletes messages that are 60 days old unless an affirmative action is taken to archive emails by the user. Do you believe this system is conducive to appropriate oversight of the FBI? Are there any problems that could arise if a message has been automatically deleted that may be necessary after the 60-day window?

Response:

The FBI's Exchange email system has three locations for message storage. The first location is an enterprise repository that stores a copy of every email message created and sent. Messages remain in the enterprise repository for 90 days. Messages older than 90 days are automatically deleted from the repository pursuant to Records Management Division (RMD) policy.

Messages are also stored in personal mailboxes. Every FBI employee has a personal mailbox, and each employee is responsible for managing that personal mailbox (deleting and archiving messages, organizing messages within files, etc).

Messages stored in a user's personal mailbox are not deleted after 90 days. Only the user can delete messages from the personal mailbox.

The third location in which mail messages are stored is the personal archive file (PST file). Users can move mail out of their personal mailboxes and into PST files. The movement of files from a user's personal mailbox to a PST file is controlled by the user, as is the deletion of files from a user's PST file. PST files have no set retention time. Messages within a PST file are deleted only if the user takes action to delete them.

25. Committee staff was briefed by the Foreign Terrorist Tracking Task Force (FTTTF) that 2 terrorists a week are detected in the United States and those leads are forwarded to the Joint Terrorism Task Force (JTTF). We know from the FTTTF representative who briefed our staff that 2 of the 9/11 hijackers were on the terror watch list, but the information was not communicated to the JTTF. Have you identified the cause of the breakdown, and taken steps to avoid its reoccurrence?

Response:

Before the attacks of 9/11/01, multiple terrorist watchlists were maintained by various Federal agencies without review by or coordination with other agencies. The two 9/11 hijackers referenced in the question were on the Department of State (DOS) watchlist referred to as TIPOFF at the time of the attacks, but the FBI was not aware of this. Following the 9/11 attacks, HSPD 6 (9/16/03) mandated the creation of the Foreign Terrorist Tracking Task Force (FTTTF) and the Terrorist Screening Center (TSC) to ensure watchlists and terrorist tracking efforts are coordinated throughout the Federal government.

The TSC was created to systematize the Government's approach to terrorist screening and to the maintenance of secure, consolidated terrorist identity information. The TSC shares watchlist information with Federal, state, local, territorial, and tribal law enforcement agencies and with others in the IC.

The FTTTF was created to provide information that helps to keep foreign terrorists and their supporters out of the United States or that leads to their location, detention, removal, prosecution, or other appropriate action. The FTTTF uses innovative techniques to provide the information necessary to fill gaps relating to the location of known or suspected terrorists and terrorism supporters. Like the TSC, the FTTTF shares this information with Federal, state, local, territorial, and tribal law enforcement agencies and with others in the IC.

26. A June 2005 OIG report entitled "A review of the Terrorist Screening Center" found that the watch list could be missing names, some names might be designated at inappropriate threat levels and that the FBI hasn't given other agencies full access to its watch list. Is this still a problem?

Response:

The TSC is charged with developing an accurate watchlist of known and suspected terrorists. These identities and the derogatory information describing their specific nexus to terrorism are passed to the TSC through the watchlist nomination process by either the National Counterterrorism Center (NCTC) (for international terrorism subjects) or the FBI (for domestic terrorism subjects).

Upon the receipt of an NCTC or FBI nomination, the TSC conducts an individual review of the available information, including the derogatory information on which the nomination is based. If this information supports placement on the watchlist, the identity is included on all watchlists for which it qualifies, including the Violent Gang and Terrorist Organization File (VGTOF), the Transportation Security Administration (TSA) Selectee and No Fly lists, DHS' Interagency Border Inspection System, the DOS Consular Lookout and Support System, as well as to the Canadian and Australian governments through programs called TUSCAN and TACTICS, respectively. Each of these lists has specific minimum criteria for inclusion. For example, inclusion on TSA's No Fly list requires that the nomination contain a full date of birth in addition to other specific derogatory information, and citizenship status affects inclusion in TUSCAN and TACTICS.

The FBI requires that all subjects of domestic terrorism full investigations be watchlisted and that all subjects of international terrorism preliminary or full investigations be nominated for watchlisting (watchlisting the subjects of domestic terrorism preliminary investigations is at the discretion of the field office involved). Consequently, these identities will also be included in the other watchlists for which the subject qualifies. From these lists, other agencies have access to information regarding FBI subjects.

27. In a recent article, Judge Richard Posner stated, "We would probably be better off with a different reorganization (of intelligence) with ... a domestic intelligence agency separate from the FBI." (Posner, 04/11/06.) Do you disagree with this assessment? Why do you disagree with him?

Response:

The FBI believes there is no reason to separate the functions of law enforcement and domestic intelligence. On the contrary, combining law enforcement and

intelligence affords us ready access to every weapon in the government's arsenal against terrorists, allowing us to make strategic and tactical choices between the use of information for law enforcement purposes (arrest and incarceration) or intelligence purposes (surveillance and source development).

The benefits of this approach have been clearly borne out. Since 9/11/01, the FBI has identified, disrupted, and neutralized numerous terrorist threats and cells, and we have done so in ways an intelligence-only agency like the United Kingdom's MI-5 cannot.

Because of its personnel, tools, and assets, the FBI is uniquely suited for the counterterrorism mission. These resources include:

- A worldwide network of highly trained and dedicated SAs;
- Intelligence tools to collect and analyze information on threats to national security;
- Law enforcement tools to act against and neutralize those threats;
- Expertise in investigations and in the recruitment and cultivation of human sources of information;
- Longstanding and improving relationships with those in state and local law enforcement, who are the intelligence gatherers closest to the information we seek from these communities; and
- Nearly a century of experience working within the bounds of the United States Constitution.

For these reasons, the FBI believes the United States is better served by enhancing the FBI's dual capacity for law enforcement and intelligence gathering/analysis than by creating a new and separate domestic intelligence agency, which would constitute a step backward in the war on terror, not a step forward.

Experience has taught the FBI that there are no neat dividing lines distinguishing criminal, terrorist, and foreign intelligence activities. Criminal, terrorist, and foreign intelligence organizations and activities are often interrelated or interdependent. FBI files contain numerous examples of investigations in which information sharing between counterterrorism, counterintelligence, and criminal intelligence efforts and investigations was essential to the FBI's ability to protect the United States from terrorists, foreign intelligence activities, and criminal efforts. Some cases that begin as criminal cases become counterterrorism cases,

and vice versa. The FBI must sometimes initiate parallel criminal and counterterrorism or counterintelligence cases to maximize the FBI's ability to identify, investigate, and address threats to the United States. The success of these cases is entirely dependent on the free flow of information between the respective investigations, investigators, and analysts.

That said, the FBI is in the process of adopting some aspects of MI-5. One of the benefits inherent in an intelligence organization like MI-5 is its ability to establish a "requirements" process where current intelligence requirements are reviewed (whether they be terrorism, international crime, cyber crime, etc.) and knowledge gaps are identified. The next step is to get the intelligence collectors (in this case, FBI SAs from around the country) to fill in those gaps. The FBI has adapted and is incorporating this kind of intelligence requirements process, not just with respect to terrorism but for all programs. This process is invaluable in helping to better prioritize FBI resources and to identify the gaps in understanding.

In arguing that a separate domestic intelligence agency should be created, Judge Posner asserts that "the bureau's conception of intelligence is of information that can be used to obtain a criminal conviction." We emphatically disagree with this assertion. In the nearly 4½ years since the attacks of 9/11/01, the FBI has undergone a dramatic transformation from a law enforcement agency focused on investigating crimes after the fact into an intelligence and law enforcement organization focused largely on preventing terrorist attacks. We have entered an era of unprecedented information sharing among the law enforcement and intelligence communities and we are continuing to build on our success in strengthening our intelligence capabilities.

The most recent step in the FBI's evolution is the establishment of its National Security Branch (NSB), which combines the capabilities, resources, and missions of the Counterterrorism Division (CTD), the Counterintelligence Division (CD), and the Directorate of Intelligence (DI) under one leadership umbrella. The NSB will build on the FBI's strengths, ensure the integration of national security intelligence and investigations, promote the development of a national security workforce, and facilitate a new level of coordination with others in the IC.

Three major assessments of the FBI's intelligence capabilities have agreed that the FBI should retain its domestic intelligence responsibilities: the report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), the assessment by the National Academy of Public Administration (NAPA) of the FBI's transformation, and the report of The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission). In its March 2005 report, "Transforming the FBI: Progress and Challenges," the NAPA Panel on FBI Reorganization wrote:

"This Panel, like the 9/11 Commission, is convinced that the FBI is making substantial progress in transforming itself into a strong domestic intelligence entity, and has the will and many of the competencies required to accomplish it. That Panel recommended that the FBI continue to be the key domestic intelligence agency responsible for such national security concerns as terrorism, counter-intelligence, cyber, and transnational criminal activity."

The WMD Commission also examined the FBI's intelligence program and concluded in March 2005 that it had been significantly improved since 9/11/01. The commission rejected the need for a separate agency devoted to internal security without any law enforcement powers, recognizing that the FBI's hybrid intelligence and investigative nature is one of its greatest strengths and emphasizing the importance of the ongoing effort to integrate intelligence and investigative operations. At the same time, the commission noted that the FBI's structure did not sufficiently ensure that intelligence activities were coordinated with the rest of the IC. Accordingly, the commission recommended the creation of a "National Security Service." In response to the President's directive endorsing that recommendation, the FBI created the NSB.

28. It has been alleged that some of the new FBI analysts were administrative assistants at the FBI who were promoted to the analyst position, without an actual change in their job positions or responsibilities. Is this allegation true?

Response:

This is not true. The FBI is hiring Intelligence Analysts (IAs) who possess critical skills and meet both educational and professional qualifications. The FBI's internal applicants for IA positions must meet the same qualifications as external candidates. FBI metrics indicate that qualification standards for IAs have steadily increased in terms of both education and critical skills. More than 90% of all FBI IAs hired within the last 2 to 5 years have bachelors' degrees and more than 48% have advanced degrees. New FBI IAs also possess critical skills in such areas as Islamic studies, international banking, analytical studies, and computer science.

29. Given Choicepoint's substantial history of compromised databases, why has the FBI chosen to contract out information analysis to them?

Response:

The FBI awarded a 5-year, fixed-price contract to i2, Inc., a subsidiary of ChoicePoint, on 12/1/05. ChoicePoint issued a press release announcing this contract on 4/3/06, which created some confusion as to whether the contract was for ChoicePoint data services or for i2 analytical tools. In fact, this contract is

solely for i2's software applications and analytical tools, and not for ChoicePoint data services. These i2 applications and tools include software licenses, software upgrades, technical support for i2's primary product, the "Analyst's Notebook," a scaled-down version of i2's "Visual Notebook," and related tools. The "Analyst's Notebook" is a link-node analysis tool that has proven highly useful in counterintelligence, counterterrorism, and criminal investigations that involve large volumes of data.

The FBI also continues to use ChoicePoint's data services, and we are committed to continuing to use this information responsibly. In pursuit of our national security and criminal investigative missions, FBI SAs and analysts must have access to the same types of information, with appropriate safeguards, to which an average private investigator or paralegal can subscribe. Commercial databases such as ChoicePoint contain public information (which includes information obtained from public sources) as well as proprietary information that is privately owned and commercially available at the discretion of the owner. This information is available to the FBI from the same sources that provide it to the commercial databases. What commercial databases offer their customers, including the FBI, by contract is a consolidation of this information so that, rather than going to multiple databases for this information, it can be obtained through one or two searches.

The FBI's contracts with commercial databases do not, in any respect, undermine the FBI's obligation to comply with all federal laws that protect an individual's privacy including, among others, the Privacy Act, the Right to Financial Privacy Act, and applicable provisions of the federal tax code. In other words, the FBI can only collect and retain data available from commercial databases in compliance with applicable federal law.

The United States Constitution and the United States Congress, through legislation, carefully delineate acceptable conduct in law enforcement investigations and intelligence activities. The FBI has an unwavering commitment to adhere to those requirements, as well as those mandated by federal regulations and the Attorney General's Guidelines. Whether the work is performed manually or in an automated fashion, that commitment does not change. The FBI exercises due diligence to ensure that the use of public source data is in furtherance of the FBI's mission and consistent with applicable privacy laws, regulations, and policies.

30. The turnover rate for the position of Executive Assistant Director (EAD) for Counterterrorism and Counterintelligence has been remarkably high, with a total of six over the past five years. This month, current EAD Gary Bald announced his retirement after only six months on the job. This turnover is clearly harming the efforts of the FBI to

improve its counterterrorism and counterintelligence activities. Will you require the next EAD, prior to his or her promotion, to agree to stay on for at least two years, if not more? If not, why not? Will you require other potential FBI leaders to make similar agreements?

Response:

We disagree that the turnover in the position of Executive Assistant Director (EAD) for Counterterrorism and Counterintelligence has harmed the efforts of the FBI to improve those programs. The success of the FBI's national security programs is not dependent upon a single person. The leadership teams in both CTD and CD have decades of operational experience and have successfully developed effective programs at Headquarters and throughout the field offices. With regard to the promotion of future executives, minimum time commitments may be discussed but are not enforceable.

31. The FBI is perhaps the only law-enforcement agency in the country that doesn't use standardized promotional exams or any other objective criteria in selecting managers for advancement. Why not?

Response:

The FBI does, in fact, use standardized promotional assessments in selecting managers for advancement. The FBI has recently implemented a new, three-phased standardized and professionally validated promotion system, called the SA Mid-Level Management Selection System (SAMMSS). This promotion system, which was recently implemented as part of a settlement agreement (Johnson et al v. Ashcroft, Civ. No. 93-0206 (DDC)), emphasizes the managerial and leadership skills required to lead others in the execution of the FBI's National Security and Law Enforcement Mission. These managerial and leadership skills were established as essential for all GS-14 and GS-15 SA mid-level managerial positions through three separate job analyses conducted in conformance with professional and legal guidelines, including the 1978 Equal Employment Opportunity Commission Uniform Guidelines on Employee Selection Procedures. The FBI especially wanted to emphasize the importance of leadership and management in its managerial cadre; therefore, the promotion system focuses on both the technical knowledge and the managerial and leadership skills required to perform any managerial job. The eight core managerial competencies identified through the three job analyses upon which the promotion system is based include: leadership, interpersonal ability, liaison, planning and organizing, problem solving, flexibility and adaptability, initiative, and communication. These competencies are measured and evaluated in a standardized manner throughout the different phases of the SAMMSS.

32. The FBI's Office of Professional Responsibility (OPR) and the Internal Investigations Section (IIS) of the FBI Inspections Division seem to be having problems doing their jobs. Twice recently, in cases involving 1) the murder of Assistant US Attorney Jonathan Luna and 2) potential retaliation against FBI agent Mike German, the OPR and the IIS mischaracterized these cases as involving only "performance issues" rather than "misconduct issues," only to have the Department of Justice's Inspector General contradict them. Why is this happening? How many times in the last five years has the IG reached opposite conclusions than an FBI investigative unit? If the FBI is unable to police itself, do you feel that this task should be taken away from it and given to the IG?

Response:

Director Mueller commissioned a comprehensive review of the FBI's internal disciplinary process in May 2003 to be led by former United States Attorney General and Federal Judge Griffin B. Bell and by former FBI Associate Director Dr. Lee Colwell. The Bell Colwell study looked at all aspects of the FBI's internal disciplinary process, including its structure, responsibilities, standards, and processes. A final report was provided to the FBI in February 2004 and its recommendations were adopted. Organizational changes included the April 2004 transfer of the Internal Investigations Section (IIS) from the FBI's Office of Professional Responsibility (OPR) to its Inspection Division. Other changes, including policy directing that an OPR matter will not be discontinued or closed when the subject retires or resigns during the pendency of an investigation if necessary to protect the FBI's institutional interests, became effective in November 2004. The cases cited in the question were investigated and adjudicated before implementation of the Bell Colwell recommendations.

The Inspection Division's IIS does not maintain a record of its differences with DOJ's Office of the Inspector General (OIG). It is the FBI's understanding that the OIG also does not maintain a record of these differences. Under the current structure, the IIS coordinates closely with the OIG but the FBI and the OIG generally do not investigate the same cases and, therefore, seldom have the opportunity to reach different interpretations or investigative conclusions. While longstanding DOJ policy does not permit the FBI to comment on the outcomes of such investigations, in neither of the two cases cited in the question did the OIG and the FBI examine the same conduct of the same individual and reach different conclusions. Under the current structure, the OIG reviews all allegations of misconduct by FBI personnel, chooses to investigate a small fraction of those allegations, and refers the remainder back to the IIS for independent evaluation and appropriate action. The OIG also monitors the FBI's internal investigations as appropriate and can assume responsibility for an ongoing investigation at any time. When the OIG investigates an FBI employee, the IIS and other FBI entities cooperate with the OIG and assist to the extent the OIG deems appropriate.

Because the OIG can intervene at all these points, the OIG does, in fact, "police" the FBI.

The FBI is completely able and willing to "police itself" and it cooperates fully in OIG investigations of FBI personnel. The FBI maintains an entire Section dedicated solely to internal investigations, and that Section can and does draw on others in the FBI to support its mission, including Supervisory Special Agents (SSAs), Assistant Special Agents in Charge (ASACs), Unit Chiefs, and even Senior Executive Service (SES) officials. The FBI's OPR is dedicated solely to the independent adjudication of internal investigation results. When appropriate, other FBI Divisions conduct criminal investigations of FBI personnel. For decades, whether a matter was as relatively minor as the inadvertent loss of identity documentation or as significant as espionage, the FBI has "policed itself" with a total commitment to professionalism, thoroughness, and objectivity.

33. The Department of Justice Reauthorization Act of 2005 directs the FBI to establish a task force to combat organized retail theft. Since this bill's passage, the FBI has seemingly done little to implement this task force. Is there a reason for the FBI's inaction?

Response:

The FBI has been actively engaged in establishing a task force to combat organized retail theft. Section 1105 of the Violence Against Women and DOJ Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960, 3092 (1/5/06), directs the Attorney General (AG) and the FBI, in consultation with the retail community, to "provide expertise to the retail community for the establishment of a national database or clearinghouse housed and maintained in the private sector to track and identify where organized retail theft type crimes are being committed in the United States."

The FBI has engaged in a number of specific actions in satisfaction of this requirement. Upon enactment of the legislation, the FBI formed a working group with the National Retail Federation and consulted with members of the retail community to ensure the specific needs of the retail community shaped the design of the national clearinghouse and the composition of the task force. The FBI working group identified two existing private databases, each vying to be the "national database" used by the industry and law enforcement. One database, the Retail Loss Prevention Intelligence Network, was launched in December 2005 by the National Retail Federation, which developed the database in conjunction with the FBI's Major Theft Unit. DOJ and the FBI's OGC, Budget Unit, and Major Theft Unit continue to conduct research to determine the eventual structure of the "national database", the composition of the task force, and the specific

requirements for accessing and utilizing funds appropriated for Fiscal Years (FY) 2006-2009.

34. To facilitate CALEA implementation, Congress appropriated $500 million to reimburse carriers for the direct costs of modifying systems installed or deployed on or before January 1, 1995. (CALEA is the Communications Assistance for Law Enforcement Act, which was passed in 1994 at the request of the FBI to enable law enforcement to conduct electronic surveillance on the new technologies and wireless services then in existence.) Approximately 90% of this money has been spent already; there is only $45 million remaining. However, according to the IG, the FBI is determined to spend the remaining $45 million, even though the IG feels that is no longer appropriate or effective. Does the FBI believe that this money should be spent? If so, why? Does the FBI feel that CALEA has been successful overall?

Response:

Electronic surveillance forms the foundation for many of the FBI's criminal and terrorism-related investigations. In October 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) to protect national security and public safety by ensuring that changes in telecommunications technology would not compromise law enforcement's ability to conduct authorized electronic surveillance. Pursuant to CALEA the FBI balances three key goals: 1) preserving a narrowly focused ability to conduct authorized intercepts; 2) protecting privacy in light of increasingly powerful technologies; and 3) avoiding impediments to the development of new communications services and technologies.

In its March 2006 audit report regarding CALEA's implementation, DOJ's OIG recommends that the FBI re-examine *how* it plans to expend the remaining funds. While the report does not comment on either the appropriateness or effectiveness of spending the remaining funding, it does offer a list of factors the FBI should consider in determining how to spend the remaining funds. Understandably, the OIG's primary concern is that these expenditures fund efficient and effective technical solutions.

CALEA allows the reimbursement of industry costs for retrofitting existing equipment. Challenging and complex negotiations, coupled with a novel payment structure, resulted in the FBI's expenditure of approximately $450 million to cover costs originally estimated by the industry to be well over $4 billion. The FBI has managed the reimbursement process carefully, and will continue this careful stewardship of CALEA funds, expending the remaining resources to ensure the greatest possible benefit to law enforcement while honoring CALEA's reimbursement eligibility constraints.

For the first time, the most extensively deployed telecommunications services (traditional circuit-switched land line and wireless services) comply with technical standards that meet the electronic surveillance needs of law enforcement. The FBI worked with Federal, state, and local law enforcement to identify the capabilities required to intercept modern telephone services, and developed from that information standards that address the capabilities required by CALEA. The FBI continues this coordination and works with the relevant services to ensure these standards work with new and emerging communications services. For example, these standards have allowed law enforcement to address: the migration of criminal users to wireless telephones; the shift in the vast majority of Title III intercepts to wireless telephones; and the advent of new Voice over Internet Protocol and broadband access services. Additional technical standards, currently in various stages of development, will address voice services over cable, wireless data access services, and wireline Internet Protocol network access services. Both the existing and the developing standards have required extraordinary liaison and interaction among a diverse group of law enforcement agencies, other government agencies, telecommunications carriers, and telecommunications equipment manufacturers and are clear indications of CALEA's success.

Questions Posed by Senator Grassley

35. This March, a New York grand jury accused former Special Agent Lin DeVecchio of giving secret information to his informant, which led to the murders of four individuals in the 80s and early 90s. Following similar scandals involving mafia informants in Boston and former FBI agents John Connolly and H. Paul Rico, new informant guidelines were developed to ensure that similar problems did not recur.

a. Have the current informant guidelines been re-evaluated in light of the allegations against DeVecchio? If so, what additional changes may be considered in light of the allegations against DeVecchio?

Response:

Confidential informants and other confidential human sources are critical to the FBI's ability to carry out its counterterrorism, national security, and criminal law enforcement missions. A source may have a singular piece of information we could not otherwise obtain, enabling us to prevent a terrorist act or a crime or to apprehend a fugitive. It is important that the FBI have a vigorous and effective human source program that complies with legal and Departmental requirements.

Because of the importance of this program, several months ago the FBI's DI initiated a comprehensive review and revision of our HUMINT program in

conjunction with DOJ. As one part of the re-engineering project, the FBI is working with DOJ to draft revised AG Guidelines governing source operations and to develop new internal manuals. The Validation Standards Manual details the implementation of a comprehensive, Bureau-wide validation process that has been reviewed by DOJ and complies with the standards developed by the Director of National Intelligence (DNI). In addition to requiring the validation of every source and every relationship between an SA and a source on a regular and consistent basis, the revised validation process will be streamlined and automated through a new technology application. By automating the administrative aspects of human source operations, the FBI will improve compliance with AG Guidelines and reduce human error.

b. If the allegations against DeVecchio are proven, please explain which provisions of the current informant guidelines that were not in effect at the time of his actions might have prevented his misconduct or brought it to light earlier.

Response:

The existing AG Guidelines Regarding the Use of Confidential Informants provide for substantial oversight of the FBI's use of informants, including annual internal reviews of informant files and external reviews of long-term informants by DOJ's Confidential Informant Review Committee (CIRC). These AG Guidelines expressly prohibit law enforcement agents from interfering with criminal investigations involving confidential informants and provide specific guidance concerning prohibited transactions and relationships. As indicated in response to subpart a, above, the FBI is currently re-engineering its HUMINT program. This re-engineering effort and the implementation of forthcoming validation procedures will allow for a thorough and comprehensive review of the classifications of all sources being operated in the FBI. Part of the re-engineering effort includes a review of the current CIRC process, including the current procedure under which a source can have a designated classification that would not be reviewed by the CIRC.

c. Please provide a detailed description of the nature and extent of previous internal investigations into DeVecchio's relationship with Gregory Scarpa Sr., including (1) the origin of the allegations, (2) the factual findings of the investigations, and (3) an explanation of the basis for any conclusion to impose or not impose discipline on DeVecchio for alleged misconduct.

Response:

In 1995, the United States Attorney's Office for the Eastern District of New York alleged in an ex parte court filing that SA DeVecchio had unlawfully provided

confidential law enforcement information to an informant involved in organized crime in New York. These allegations were reviewed and investigated by DOJ's Public Integrity Section and the FBI's OPR. In September 1996, the Public Integrity Section determined that prosecution of SA DeVecchio was not warranted, and the OPR investigation was closed. SA DeVecchio retired from the FBI in October 1996. At that time, FBI policy did not provide for the continuation of internal investigations after a subject retired or resigned even if continuation would protect the FBI's institutional interests. The FBI's current policy of continuing internal investigations under those circumstances is based on recommendations resulting from the Bell Colwell review of the FBI's internal disciplinary system.

36. According to the website maintained by DeVecchio's supporters in the FBI (www. lindevecchio.com), the agents helped post a one million dollar bond to secure his release and are raising money for his legal defense. After his arraignment agents surrounded DeVecchio "in a human blanket" as he left the courtroom so that he could not be questioned by reporters. One agent wrote, "it might even be said that a few reporters received a few body checks out on the sidewalk" and that he "was never prouder to be an FBI Agent."

a. Is it appropriate for current and former FBI agents to cite their affiliation with the Bureau to lend credibility to a private effort to raise money for a defendant charged with murder? Please explain why or why not.

b. What rules, if any, govern an agent's use of affiliation with the FBI for other than official purposes?

Response to subparts a and b:

It would be inappropriate for current FBI employees to use their FBI affiliation to lend credibility to their private efforts to raise money for a criminal defendant. Internal FBI regulations generally prohibit employees, except in an official capacity, from becoming involved in any matter directly or indirectly concerning an employee or non-employee who has been arrested or is otherwise in difficulty with a law enforcement agency, from attempting to mitigate the action of any arresting officer, agency, or prosecuting officer, and from trying in any way to minimize publicity concerning such incidents. When expressing their personal views or discussing matters related to the functions of the FBI, FBI employees are cautioned to make clear that they are stating their personal opinions, not those of the FBI, especially when they have been identified as FBI employees.

In addition, current FBI employees are subject to the regulations governing federal employees generally. Pursuant to these regulations, "[e]mployees shall not use

public office for private gain." (5 C.F.R.§ 2635.101(b)(7).) Employees are also prohibited from using their Government position, title, or authority to induce others to provide any benefit to the employee or to another person, or in a manner that could be construed as implying that the FBI or another Government entity sanctions or endorses the employee's personal activities or those of another. (5 C.F.R. § 2635.702.) Federal employees also may not use, or allow the use of, their official titles or positions to further their personal fund raising efforts. (5 C.F.R. § 2635.808(c)(2).)

In contrast, former FBI employees who are no longer in federal service are not subject to these restrictions. While a federal statute (18 U.S.C. § 709) prohibits the use of the FBI's name to convey the impression that the FBI endorses a publication or production, it does not, by its terms, prohibit former FBI employees from referring to their former FBI positions to "lend credibility" to their own beliefs about a former colleague in soliciting donations on his behalf.

c. If an agent boasts about assaulting members of the press, does that constitute misconduct? What action, if any, has been taken to investigate the propriety of activities on the part of active agents who are supporting Mr. DeVecchio?

Response:

If the individual who boasted about "assaulting members of the press" was a former FBI employee at the time of the alleged offense, he/she would not be subject to the FBI's internal disciplinary process. If, however, a current FBI SA boasted of assaulting a member of the press, such conduct would be covered by the FBI's disciplinary process and would constitute misconduct. If an assault actually occurred, the SA might be terminated and/or criminally prosecuted. Even if no assault took place, such boasting by a current FBI employee would negatively impact the FBI's image. Conduct that disgraces, dishonors, or discredits the FBI or compromises the standing of the FBI, whether committed on- or off-duty, constitutes "unprofessional conduct" and is sanctionable. The sanction imposed would depend on the specific facts of the case, including the impact such a statement had on the public's confidence in or perception of the FBI, the demoralizing impact the statement had on other FBI employees, and the employee's prior disciplinary record. Because the types of misconduct that constitute "unprofessional conduct" are quite varied, the FBI's OPR is given wide latitude in determining the appropriate sanction for this offense, ranging from an oral reprimand to dismissal.

The DOJ OIG has not notified the FBI that it has received any allegations of misconduct by current FBI personnel who support Mr. DeVecchio, and the FBI is otherwise unaware of any such allegations. We have, consequently, not initiated

an investigation. Should the FBI's IIS become aware of such an allegation, it would provide that information immediately to the OIG for review. If the OIG were to refer the matter back to the FBI, the IIS would evaluate the information carefully and investigate the matter further, if appropriate.

37. During the recent sentencing hearings for convicted terrorist Zacharias Moussaoui, Harry Samit, the Minneapolis FBI agent who conducted the investigation of Moussaoui testified at length about the lack of support he received from FBI supervisors during his efforts to obtain a warrant to search Moussaoui's computer and apartment. He said that he "warned higher-ups and others in the government at least 70 times that Moussaoui was a terrorist." He described the failure of FBI supervisors as "criminal negligence, obstructionism, and careerism." This is amazing testimony from a sitting agent in one of the most important cases in FBI history.

a. What steps have you taken to ensure that Agent Samit will not face retaliation for his recent testimony?

Response:

Director Mueller is committed to ensuring the protection of FBI employees who report organizational wrongdoing and has issued multiple communications reiterating his position that reprisals will not be tolerated, nor will attempts to prevent employees from making protected disclosures. Employees who engage in reprisals or intimidation against individuals who make protected disclosures can expect appropriate disciplinary sanctions, including dismissal from the rolls of the FBI, where warranted.

While Special Agent Samit's concerns have only recently been made public as a result of the Moussaoui sentencing hearing, they have received considerable review by numerous internal and external entities since 9/11/01, including the Joint Inquiry of the House and Senate Intelligence Committees, the 9/11 Commission, and the DOJ OIG. These reviews have resulted in findings and recommendations that have been incorporated into the FBI's ongoing transformation.

b. The chapter on the Moussaoui case in the Inspector General's report on the FBI's handling of intelligence information before 9/11 was not released at the same time as the rest of the report because the criminal case against Moussaoui was still pending at the time. Now that Moussaoui has been sentenced, do you support the release of a declassified version of that chapter, so that the American public can understand better what happened?

c. What action, if any, is required by the FBI before the chapter can be released?

d. When do you expect that chapter to be released publicly?

Response to subparts b-d:

The DOJ OIG issued its completed report in November 2004. The full report, classified at the Top Secret/Sensitive Compartmented Information (SCI) level, was provided to the FBI, DOJ, Central Intelligence Agency (CIA), National Security Agency (NSA), 9/11 Commission, and Congress. At the request of members of Congress, the OIG created an unclassified version of the report. In June 2005, consistent with the rules of the United States District Court for the Eastern District of Virginia, the Court gave the OIG permission to release the sections of the unclassified report that did not discuss the FBI's investigation of Zacarias Moussaoui. The Moussaoui case concluded on 5/4/06, and on 6/19/06 the OIG released the full version of the unclassified report, which includes the Moussaoui chapter (chapter 4) and other references to Moussaoui throughout the report.

38. Agent Harry Samit's testimony provides at least some reason to believe that the horrific events of 9/11 might have been averted if FBI supervisors had listened to and supported their field agents. It also raises the question of whether too many supervisors operate by the principle that some agents describe as, "Big cases equal big problems. Little cases equal little problems. No cases equal no problems."

a. How do you identify which supervisors regularly fail to support the investigative efforts of their field agents?

Response:

FBI supervisors are subject to annual Performance Appraisals and semi-annual Progress Reviews provided by their Rating and Reviewing Officials. In addition, every three years, the FBI's Inspection Division conducts comprehensive inspections of every field office, Legal Attaché, and FBI Headquarters (FBIHQ) entity. These inspections emphasize management performance at all levels. Prior to the inspection, each employee is requested to complete an automated leadership survey regarding the two levels of management above them. The survey includes questions regarding the supervisors' competence, ethics, and support of investigations. The survey is anonymous. Every SA and 50% of all support employees are personally interviewed by the inspection staff and asked about management's support of their efforts. Investigative and source files are

reviewed, outside agency contacts are interviewed, statistical accomplishments are assessed, and a determination is made regarding each supervisor's performance.

b. What should a field agent do when a supervisor consistently fails to reward initiative or approve investigative proposals? Is there any way to report the problem without fear of retaliation?

Response:

Within a field office, an employee is free to speak to the ASAC or SAC if unable to resolve an issue with a direct supervisor. Consistent supervisory declination of investigative proposals would produce a trail of documentation, and a field SA could share this documentation with executive managers, who are encouraged to maintain "open door" policies.

The FBI's inspection process addresses supervisory effectiveness in a number of ways. A preliminary assessment of whether initiative is rewarded can be obtained through a specific inspection interrogatory that requires supervisors to list all employee awards. In addition, the pre-inspection leadership survey and employee interviews are designed to determine whether initiative and tangible results are being rewarded, whether managers' open door policies are being honored, and whether managers are otherwise effective. The file reviews conducted during field office inspections help to identify supervisors who consistently disapprove operational proposals or mismanage investigations, and field SAs have the opportunity to speak privately with inspectors during inspections.

Although the FBI can never completely eliminate an employee's fear of retaliation, factors likely to induce such fear can be reduced or eliminated. The anonymous nature of the inspection leadership survey, private interviews with the inspection staff, and executive managers who promote the proper environment all help to reduce the fear of retaliation. If an employee nonetheless believes retaliation has occurred, this may be reported to the Inspection Division's IIS or to DOJ's OIG or OPR. FBI employees are also frequently reminded through FBI-wide emails and other mechanisms that there is a procedure established under law (5 U.S.C. § 2303) and implemented by regulation (28 C.F.R. Part 27) that provides a formal avenue for an employee to seek corrective action based on a personnel action taken in reprisal for whistle blowing.

c. How does FBI headquarters measure the productivity and performance of particular field offices? To what extent does the Bureau track metrics such as frequency of electronic surveillance, number of search warrants executed, and numbers of active confidential informants as well as numbers of arrests, indictments, and convictions?

Response:

Field office performance and productivity is continuously tracked and evaluated. The recently implemented COMPASS database placed a wide variety of performance metrics on the computer desktop of every field Executive Manager and many FBIHQ Executive Managers. COMPASS enables production of reports on statistical accomplishments, resource utilization by program, confidential informant and asset data, and many other performance metrics. Regular reports are generated that enable managers to track progress in specific areas over selected time frames, compare offices of similar size, monitor resource utilization by squad, program and office, and measure source development against specific targets. Each of the operational divisions at FBIHQ maintains data specific to field office performance in particular programs. During on-site inspections the Inspection Division compiles and analyzes all available metrics including the utilization of sophisticated investigative techniques, seizures and forfeitures, indictments and convictions, national security accomplishments, and others. This data helps form the basis of an inspection determination as to the effectiveness and efficiency of an office's investigative programs and the performance of its managers.

39. Please identify and describe any and all agent surveys or questionnaires conducted by the FBI, outside consultants, or independent entities within the last 15 years.

Response:

The FBI does not track the circulation of surveys or questionnaires to its employees. If the Committee is interested in a particular survey or questionnaire, we will make every effort to locate it.

40. The Inspector General recently completed his report on allegations by former ICE/SAC Houston, Joseph Webber that the FBI inappropriately delayed a wiretap request on a criminal suspect in a terrorist financing case. The report has been classified secret. Mr. Webber, who reviewed a draft of the report, has told my office that passages critical of certain FBI officials were originally marked "unclassified," but had later been changed to "secret" even though they contain no information that would reveal sources or methods of gathering intelligence.

a. The Inspector General provided a copy of the draft report to FBI headquarters for classification and sensitivity review prior to seeking FBI comment on the substance of the report. Please describe the process that the FBI followed in this case to make classification decisions about the IG report and identify any instance where the procedure differed from that followed in the review of other IG reports.

Response:

The classification and sensitivity review process for this draft report was consistent with the process for other draft reports. The FBI received the original draft from the OIG as a classified document. Upon receipt, the draft report was electronically scanned. This electronic copy was distributed to RMD's Classification Unit to perform the classification review. Additionally, the technical/subject matter experts in CTD, OGC, and other relevant parties were tasked to review the draft for factual accuracy and sensitivity issues. All parties concurrently reviewed the report and provided comments and corrections, if any, to the External Audit Management Unit, Audit, Evaluation and Analysis Section, Inspection Division. The Classification Unit compiled and reviewed the sensitivity comments and content concerns for comparison to the classification issues identified in its initial review of the draft document. CTD was consulted on items where clarification was needed to complete the classification review. The final sensitivity and classification review comments, as well as technical/factual accuracy concerns, were forwarded to OGC, and the Special Counsel to the Director for final review prior to release to the OIG. The Assistant Director of the Inspection Division reviewed and signed the formal response. Inspection Division personnel transmitted the response to the OIG.

b. Are such reports reviewed solely by a classification unit in headquarters or is it disseminated to the subjects mentioned in the report? Please describe who typically participates in the classification decision, and identify who is ultimately responsible for the final classification decision.

Response:

The report was distributed to RMD's Classification Unit, the technical/subject matter experts in CTD, OGC, and other relevant parties. Final, official classification authority rests with the Classification Unit, and sensitivity concerns, as well as factual accuracy and technical issues, are the responsibility of the technical/subject matter experts in the affected division -- in this case, CTD. The Classification Unit may make recommendations or express concerns to the affected division concerning law enforcement sensitive content, references to or including information from other agencies, etc., but the Classification Unit primarily reviews OIG drafts and proposed FBI responses for classification pursuant to Executive Order 12958, as amended, and in accordance with FBI and DOJ policies.

c. Do you believe that it would present an inappropriate conflict of interest to give FBI officials who are the subject of criticisms in an IG report the ability to censor the public version of that report? Please explain why or why not.

Response:

Neither with regard to this report nor any other OIG product did the FBI "censor the public version of the report." We agree that information should not be marked SECRET to protect individuals or the FBI from criticism or embarrassment. Classification reviews are conducted to ensure compliance with Executive Order 12958, as amended, and FBI and DOJ policies. These reviews are professional and objective.

d. Were any FBI officials mentioned in this report allowed to make decisions, directly or indirectly, about which portions would be classified?

Response:

Although parties named in the report were allowed to review the draft and provide comments on sensitivity and technical/factual accuracy, official classification decisions were made by the Classification Unit.

e. Please list all of the FBI officials who reviewed the report for classification purposes and when each review occurred.

Response:

Pursuant to the release of the draft by the OIG on January 27, 2006, the Classification Unit performed the official classification review in February 2006 (reported on 02/07/06). The Acting Unit Chief and her supervisor oversaw the classification review and approved the classification.

41. Earlier this year, the Inspector General completed his report into the allegations for former FBI Special Agent Michael German. The Inspector General found that after he wrote an internal whistleblower letter about the mismanagement of an undercover operation in Tampa, he was retaliated against. FBI Undercover Unit Chief Jorge Martinez vowed that German would never work another undercover case and blocked German from continuing to teach other agents at FBI training sessions. The IG also found that some unknown FBI official altered official records with correction fluid in order to undercut German's claims.

a. What steps has the FBI taken to identify the individual who altered official records with correction fluid?

Response:

The DOJ OIG referred its findings to the FBI's OPR, where they are being adjudicated. We do not anticipate undertaking additional investigative steps in response to the OIG's referral.

b. What are the maximum consequences that Unit Chief Martinez may face for retaliating against German?

Response:

Under the FBI's adjudicative guidelines, the maximum penalty for an employee who is found to have retaliated against a whistleblower is dismissal.

c. Please list all FBI personnel who have been disciplined for whistleblower retaliation and provide a brief description of each case, including a description of the punishment imposed.

Response:

Since the promulgation of regulations governing whistleblower protection for FBI employees in November 1999, one employee has been disciplined for whistleblower retaliation. That employee, an ASAC, was found to have retaliated against an SA based on the SA's protected disclosure. Investigation of this matter was initiated by DOJ's OPR in June 2003 and it was adjudicated by the FBI's OPR in February 2005 under the disciplinary system in place before implementation of the Bell Colwell recommendations based on the precedent relied upon at that time. The ASAC exercised his right to appeal, and the FBI's Appellate Unit vacated the 3-day suspension. The FBI's OGC has since opined that the Appellate Unit's analysis of DOJ's whistleblower regulation was flawed, but there is no vehicle for reversing an appellate determination under these circumstances. Under the present penalty table, the violation would have resulted in a penalty ranging from a 10-day suspension to dismissal.

d. When do you expect a final decision to be made about punishment for Martinez and will you please notify the Committee about what action is taken when that occurs?

Response:

The FBI's OPR is currently adjudicating the matters referred to it by DOJ's OIG. The FBI does not routinely provide information concerning the outcome of

individual personnel matters. We are willing to discuss other methods of accommodating the Committee's legitimate oversight requests.

e. On February 3, 2006, I joined with Senator Specter and Senator Leahy in sending a letter requesting copies of documents relating to the Michael German matter. We are still waiting for a complete response from the FBI. Why has the request been delayed so long and when will we receive copies of the documents we requested?

Response:

The Committee's 2/3/06 letter requesting documents concerning the Michael German matter was addressed to the DOJ OIG, which referred the request for FBI documents to the FBI. On 4/28/06, the FBI made an initial release of material to the Committee and advised that we would supplement that production when our review of the remaining material was complete. The FBI completed its response by letter to the Committee dated 7/27/06.

42. During the investigation of the death of Assistant U.S. Attorney Jonathon Luna, agents in the Baltimore FBI office aggressively questioned one of its own female field agents who knew Luna. The agent later complained about the nature of the questioning and claimed that her laptop computer was searched without her consent. During an internal investigation of the complaint, FBI agents reportedly gave contradictory statements about the interrogation and unauthorized search. However, the FBI closed the matter as merely a "performance issue." The IG reviewed that decision and determined that it should have been treated as a misconduct issue and that the allegations against Smith-Love should have been referred to the Office of Professional Responsibility (OPR).

a. There has apparently been no criminal investigation to determine whether any FBI agents gave false statements during their interviews by the Internal Investigations Section. Why not? Isn't it crucial that the FBI get to the bottom of issues that call into question the truthfulness of its agents?

Response:

The FBI remains committed to fairly and impartially investigating allegations that call into question the candor and truthfulness of all FBI employees; however, we do not believe that differences in witness statements necessarily raise issues of candor or truthfulness.

The DOJ OIG review of the FBI's complaint investigation resulted in a recommendation that the underlying investigation be forwarded to the FBI's OPR for adjudication. The FBI adopted this recommendation, and the results of the original investigation as well as the OIG report of investigation were forwarded to

OPR for adjudication. The OIG found the facts of the matter sufficiently established for adjudication and did not recommend that additional investigation of the underlying matter be conducted. Following issuance of the OIG report, the original complainant, as well as one of the subjects of the underlying internal inquiry, made a number of allegations, including that the other had made false statements in the underlying inquiry. Inasmuch as at least one of the employees claimed "whistle blower" status, consistent with FBI policy, their letters were referred by the FBI to the DOJ OPR and DOJ OIG for handling. The DOJ OPR deferred to the DOJ OIG for consideration of the matter. The OIG responded to the FBI advising that the core allegations raised in the employees' letters involved issues that had already been investigated by IIS and/or the OIG and were ready for review and adjudication by OPR. Accordingly, no further investigation of the underlying matter was conducted.

b. After the IG intervened to ensure that OPR reviewed the matter as a potential misconduct issue, OPR reportedly determined that there was no misconduct. Please provide a detailed explanation of the basis for OPR's conclusion that no misconduct occurred in this case.

Response:

OPR substantiates allegations of misconduct based on a preponderance of the evidence. To reach a finding of misconduct, OPR must determine that a policy, law, or regulation has been violated. In this instance, OPR reviewed witness statements and other evidence contained in the investigative files and determined that the preponderance of the evidence did not support a finding of misconduct, including false statements or lack of candor.

c. What is Jennifer Smith-Love's current position with the FBI? When was she promoted to that position?

Response:

Ms. Love's current position with the FBI is Section Chief in CTD. She was promoted into that position, which is within the SES program, effective 01/03/05.

d. Please describe FBI policy with regard to promotions of employees with pending misconduct allegations?

Response:

The general policy regarding promotion of an FBI employee into or within any mid-management or SES position requires an administrative review of records by

the FBI's Office of Equal Employment Opportunity Affairs, Security Division, Inspection Division, and OPR, and by the DOJ OIG. In addition, for SES positions, record checks are conducted by DOJ's OPR and Criminal Division. These checks span the employee's entire FBI career for SES candidates and the previous 3 years for non-SES positions. Prior to any selection, the results of these record checks are considered by the relevant career board and the Director. The Director retains the authority to make final selections.

e. Did Smith-Love receive a promotion before the complaint against her was properly resolved? Please explain.

Response:

As is typically done before promotion to the SES, an administrative records check was conducted before Ms. Love was promoted to the position of CTD Section Chief. That check revealed that DOJ OIG and FBI OPR inquiries were then pending related to the Luna investigation. Director Mueller was made aware of this and approved Ms. Love's promotion, which was effective 1/3/05. Several months thereafter, it was alleged that Ms. Love had made inconsistent statements in the context of the administrative reviews of the Luna investigation. Ultimately, the FBI's OPR determined that the preponderance of the evidence did not support a finding of any misconduct, including false statements or lack of candor.

43. Cecilia Woods retired from the FBI last year after being subjected to a succession of disciplinary suspensions and unwanted transfers. These followed her reporting gross misconduct by her supervisor, including that he had engaged in a sexual relationship with a paid FBI informant. After reporting these egregious acts of misconduct by her supervisor, Agent Woods alleges that she was treated as if she were the problem instead of him. Her supervisor is still employed with the FBI even though, according to Woods, he admitted to the misconduct after initially denying it to Bureau investigators.

a. According to the FBI's disciplinary guidelines, the standard penalty for an "improper personal relationship" with an informant is a seven day suspension, although it can range from a mere censure to dismissal, depending on the circumstances. Why is it appropriate for such a serious violation to have such a broad range of potential penalties?

Response:

Improper personal relationships take many forms, ranging from non-romantic, social relationships to romantic and intimate sexual relationships. Moreover, merely creating the impression that an improper relationship exists can subject an employee to discipline. Because violations vary greatly in substance and consequence, there is a need for a broad range of potential penalties. For

example, if an SA were to regularly play golf with an informant but the conduct had no effect on the prosecution of a case, such behavior would be far less serious than an SA's involvement in a romantic relationship with an informant in which the informant's credibility was destroyed and the underpinnings of the criminal case irreparably compromised. A broad range of disciplinary options must be available to accommodate the many-faceted forms of this disciplinary infraction.

b. Please explain why the FBI should not have a zero-tolerance policy with regard to agents engaging in sexual activity with informants. Would you consider implementing such a policy?

Response:

The FBI does not tolerate SAs engaging in sexual activity with informants. The FBI's disciplinary code prohibits SAs from engaging in social, romantic, or intimate relationships with sources. It further provides that an employee will be disciplined for: (1) engaging in an improper personal relationship, or, (2) without authorization, engaging in conduct that would cause the reasonably prudent person to believe that there is an improper relationship. The sanctions available for engaging in sexual activity with informants include substantial periods of suspension and termination.

c. Please provide a detailed description of the investigations, conclusions, and actions taken against Cecilia Woods' former supervisor.

Response:

In 2000, the FBI opened an administrative inquiry pertaining to Ms. Woods' former supervisor. That administrative review substantiated allegations that the former supervisor had engaged in misconduct and he received a 14-day suspension. Before OPR concluded its adjudication of the matter, the supervisor was removed from his GS-15 position and reassigned to a GS-13 position. OPR's final adjudication letter refers to his reassignment.

d. Have any of those conclusions been re-examined in light of her former supervisor's deposition testimony in her EEOC case, in which Woods alleges he admitted to sexual activity with an individual who was a paid informant and a foreign national?

Response:

The FBI is a party in a pending administrative proceeding relating to the allegations raised by Ms. Woods. Given the pending status of this proceeding, it

would be inappropriate to comment on information developed through this confidential process.

44. The FBI recently announced the retirement of Gary Bald, head of the FBI's National Security Service. Mr. Bald had only been in this position for only eight months. The FBI's previous Director of Intelligence held that position for less than two years. The 9/11 Commission identified high turnover in key management positions as a major problem with our counterterrorism efforts.

a. Did you know when you chose Gary Bald for the position last summer that he would be retiring so soon?

Response:

Director Mueller became aware of Mr. Bald's decision to retire just prior to the public announcement on April 27, 2006.

b. Did you or anyone else involved in the decision to appoint Gary Bald as head of the National Security Service have any communications with him about his retirement plans prior to his appointment? If so, please describe the communications in detail.

Response:

Director Mueller's appointment of Gary Bald as EAD of the NSB was subject to the concurrence of the DNI and the AG. We do not believe it would be appropriate to disclose internal personnel discussions that may have occurred regarding this appointment.

c. On what date was Gary Bald first eligible to retire with full benefits?

Response:

Mr. Bald was eligible to retire with full benefits on 02/24/04.

d. On what date would he have been subject to mandatory retirement?

Response:

Mr. Bald would be subject to mandatory retirement on 02/28/11.

e. How will you ensure that the next candidate for this critical position stays long enough to provide some consistent, long-term leadership?

Response:

The FBI is presently developing succession planning initiatives targeting the SES ranks. Initiatives include inventorying the SES population's knowledge, skills, and abilities (KSAs), as well as identifying the job requirements for each SES position. This will allow the FBI to identify gaps in the SES population's KSAs to fill particular positions. With the gaps identified, the FBI can pro-actively develop a pool of qualified candidates to fill particular SES positions through training and developmental assignments. By identifying larger pools of qualified candidates, Executive Management will have greater choice from which to make selections. The FBI recruits qualified candidates for senior executive positions from all appropriate sources consistent with merit system principles.

45. In your testimony, you described the Investigative Data Warehouse (IDW), an FBI technology initiative with over 560 million FBI and other agency documents from previously stove-piped systems, accessible to almost 12,000 users.

a. How many data sources are consolidated for unified searching through IDW and how many agencies contribute data to the IDW? Please list all of the data sources and the agencies providing them.

b. Please describe the extent to which the IDW currently allows searching data contained in the information systems maintained by the Drug Enforcement Administration.

c. Please describe the extent to which the IDW currently allows searching data contained in the information systems maintained by the U.S. Secret Service.

d. Please describe the extent to which the IDW currently allows searching data contained in the information systems maintained by the U.S. State Department (other than information on lost or stolen passports).

e. Please describe the extent to which the IDW currently allows searching data contained in the information systems maintained by the Bureau of Alcohol, Tobacco and Firearms.

f. Which law enforcement organizations contribute data from their information systems to IDW other than the FBI, Immigration and Customs Enforcement, and the Financial Crimes Enforcement Network?

g. What steps are you taking to encourage other law enforcement entities to contribute data from their systems?

h. What percentage of FBI agents currently has access to IDW?

i. What percentage of FBI analysts has access to IDW?

j. What percentage of agents and what percentage of analysts with access to IDW would constitute full deployment?

k. When do you expect to reach full deployment?

l. How much would full deployment cost and how much of the total cost is covered by existing budget requests?

m. How many non-FBI law enforcement agents have access to IDW? How many of those serve on Joint Terrorism Task Forces (JTTFs)? How many do not? Please explain whether and to what extent non-FBI law enforcement agents will be granted access to IDW, including the ability to search ACS (or future FBI case-management systems) both inside and outside the JTTF-context.

n. What level of access by non-FBI law enforcement agents would constitute full deployment of IDW?

Responses to subparts a-n:

The responses to these inquiries are sensitive and are, therefore, provided separately.

46. In February, 2006, the Government Accountability Office (GAO) released a report of a study of the FBI's management of the Trilogy Project, finding over $10 million in questionable or undocumented costs. The GAO report singled out two Trilogy contractors, Computer Sciences Corporation and CACI International, Inc., for inflated spending and inadequate documentation. On March 18, 2006, the *Washington Post* published an article reporting that those same two contractors will be working on Project Sentinel as subcontractors for the general contractor, Lockheed Martin Corporation.

a. What assurances can you provide to taxpayers that any money that these contractors may owe to the government due to problems identified by GAO will be repaid before more taxpayer funds are disbursed to them under the Sentinel project?

Response:

Two vendors are common to both Trilogy and Sentinel - Computer Science Corporation (CSC) and CACI. The division of CSC that worked on Trilogy (and actually a separate firm at the time of its Trilogy work, acquired by CSC

thereafter) will not be working on Sentinel, so we anticipate little or no overlap of services or personnel. We have contracted with CACI to provide training for Sentinel, which was also the purpose of the Trilogy contract.

The FBI has strengthened its internal controls to avoid a repeat of the issues cited by the auditors with respect to all vendors. Among other things, we have improved our contract oversight in two major ways. First, the Sentinel contract has clear reporting requirements and severable deliverables. In other words, we can stop work if we are not satisfied with a contractor's progress. Second, we have structured our contract management with clearly defined roles and responsibilities, so accountable personnel are reviewing all documentation and expenses. That process will be supplemented by internal audits of our financial management, as well as by oversight from Congress and the Administration.

GSA/FEDSIM is finalizing negotiations with the GSA Deputy Assistant Inspector General (IG) for Auditing, FBI, and DCAA to have DCAA conduct an overall program audit of both task orders. The scope of the program audit will include the costs identified by GAO as potentially questionable. Upon completion of the program audit, DCAA will conduct the final closeout audit of both task orders. GSA/FEDSIM and the FBI will pursue reimbursement of any improper charges identified by that audit.

b. The GAO recommended that the FBI employ an independent third party to conduct a more complete audit of the Trilogy project. Will the FBI be implementing that recommendation? If not, why not. If so, please explain.

Response:

As noted in response to Question 11, above, it was always the intent of both the FBI and the General Services Administration's (GSA) Federal Systems Integration and Management (FEDSIM) Center to have the Defense Contract Audit Agency (DCAA) conduct final close-out audits to assess final costs, including direct and indirect labor costs. This is the appropriate means of identifying and addressing any potential overpayments to contractors. Close-out audits are designed to disclose and resolve questionable costs of the type GAO reported, as well as costs deemed unallowable under the contract. The initiation of the close-out audits has been delayed until final rates for both the prime contractors and all subcontractors have been approved by DCAA and final reconciliation is completed by both prime contractors. At that time both prime contractors will be able to submit their final invoices and DCAA will be able to complete the final closeout audit. While the prime contractors are reconciling their subcontractor costs and waiting for DCAA approval of their final rates, GSA/FEDSIM is finalizing negotiations with the GSA Deputy Assistant Inspector General (IG) for Auditing, FBI, and DCAA to

have DCAA conduct an overall program audit of both task orders. The scope of the program audit will include the costs identified by GAO as potentially questionable. Upon completion of the program audit, DCAA will conduct the final closeout audit of both task orders. GSA and the FBI will monitor the progress of the close-out audits and will ensure all areas of concern cited in the Report, including the direct labor rates charged by the contractors and their subcontractors, are thoroughly reviewed and resolved.

47. According to documents obtained by FBI agent Bassem Youssef in the course of his civil suit against the FBI, several senior FBI personnel had approved a directed transfer of Youssef to the International Terrorist Operations Section (ITOS), as late as two days before he met with you and his congressman to express concerns about the under-utilization of his native Arabic language skills and counterterrorism expertise. After that meeting, the transfer was never completed, and there has been no explanation of why not. This sequence of events presents an appearance of whistleblower retaliation. Senior FBI officials openly complained about the meeting in deposition testimony, suggesting they thought Youssef's protected disclosures to you were inappropriate. What steps are you taking to ensure that this matter receives a thorough and independent review? How can the public have confidence that no retaliation occurred in this instance?

Response:

We believe the meeting to which the question refers occurred in June 2002. At that time, the FBI was undergoing reorganization and the CTD was being restructured based on needs revealed by the 9/11/01 attacks. Among other things, a Document Exploitation project had been initiated in support of CTD's International Terrorism Operations Section (ITOS), but the project had not yet been assigned formally to CTD because the reorganization had not yet been authorized by Congress.

As indicated in public documents related to the case of Bassem Youssef v. Alberto Gonzales, et al., SSA Youssef's transfer from CD to CTD, planned before the referenced meeting, was not rescinded after that meeting. In March 2002, SSA Youssef was assigned to CD but was detailed to CTD as the manager of the Document Exploitation project, which was designed to exploit and extract information of investigative and intelligence value from foreign electronic and written media following the 9/11/01 attacks. The Document Exploitation project's main purpose was to analyze media for potential leads in the 9/11 investigation in order to prevent future terrorist attacks and to funnel relevant information to CTD's ITOS. SSA Youssef's Arabic language ability was a significant factor in his assignment to this project.

Rather than continuing his detail to CTD, the FBI planned to transfer SSA Youssef permanently to the position of CTD project manager but, in April 2002, the Document Exploitation project was in bureaucratic limbo because of CTD's ongoing reorganization. Because Document Exploitation directly supported ITOS, SSA Youssef's transfer from CD to ITOS, CTD, was the only logical designation available for the transfer to CTD at that time. The intent was that SSA Youssef would continue to perform the duties he had been performing since his assignment to the Document Exploitation project, but he would be officially assigned to CTD.

There was no action to rescind SSA Youssef's transfer or to otherwise retaliate against him after the meeting with Congressman Wolf. Because there was a legitimate business reason for the personnel action taken with respect to SSA Youssef, which was the same action contemplated before and implemented after the meeting, there is no basis for additional review.

48. According to a May 1, 2006, *Washington Post* article:

> **Many researchers and defense attorneys say [polygraph] technology is prone to a high number of false results that have stalled or derailed hundreds of careers and have prevented many qualified applicants from joining the fight against terrorism. At the FBI, for example, about 25 percent of applicants fail a polygraph exam each year, according to the bureau's security director."**

The article also cites "a comprehensive 2002 review by a federal panel of distinguished scientists" which found that "if polygraphs were administered to a group of 10,000 people that included 10 spies, nearly 1,600 innocent people would fail the test[.]"

a. Has the FBI conducted, commissioned, or reviewed scientific studies of the accuracy and effectiveness of polygraph examinations? If so, please describe them in detail. If not, why not?

Response:

For clarification, the FBI's Assistant Director for Security's comments to the reporter indicated that about 25% of applicants are disqualified as a result of the polygraph test. These results usually include admissions of information or activities that lead to a disqualification decision.

The FBI does not independently conduct or specifically commission polygraph research but it works with other federal agencies to improve polygraph techniques

and has participated in research studies with the DoD Polygraph Institute (DoDPI) which is charged with conducting research for the federal polygraph community. All DoDPI research is available directly from DoDPI.

b. What is the FBI's estimated rate of false results on polygraphs used for employment screening?

Response:

Because scientists are unable to conduct field studies under ideal (laboratory) conditions, and the absolute truth is not always available to validate the results of polygraph examinations in actual cases, known error rates remain elusive. Although error rates can be estimated, the estimates depend upon the testing situation, the issues being tested, and the persons being tested. Empirical studies cannot be used to generalize rates of error because different polygraph examiners and examination situations will produce different error rates. A major reason why scientific debate over polygraph validity yields conflicting conclusions is that the validity of such a complex procedure is very difficult to assess and may vary widely from one application to another. The accuracy obtained in one situation or research study may not generalize to different situations or to different types of persons being tested. Scientifically accepted research on polygraph testing is hard to design and conduct as evidenced by the depth of studies conducted by academic laboratories. The FBI would welcome and encourage broader research in this area.

We would offer a noteworthy data point concerning FBI internal testing of employees. Since the inception of the PSP Program in 2001, approximately 7500 counterintelligence-focused examinations have been conducted with a Deception Indicated rate of less than 1%. This result is significantly lower than the *Washington Post*'s predicted 16% failure rate.

c. Given the high rate of false results, should a "failed" polygraph alone be the basis for a negative employment decision or personnel action? How many times per year is a polygraph result the primary reason for a negative employment decision or personnel action?

Response:

We do not believe that FBI is experiencing a high rate of false positive results. Throughout the Federal polygraph community, the polygraph is considered to be an effective and acceptable screening tool and is a strong contributor in conjunction with the entire applicant process which examines the prospective employee from several standpoints. These include field investigations, records

checks and polygraph examinations. As noted earlier, polygraph results, including statements and admissions, account for about 25% of applicant disapprovals. With regard to on-board employees, a "failed" polygraph is never used as the sole basis for an adverse personnel decision. Anomalies are addressed through additional interviews and investigative work. The polygraph program does not make determinations on negative employment issues or personnel actions.

d. What steps has the FBI taken to identify more reliable alternatives to polygraph tests for ensuring the trustworthiness of current and prospective employees?

Response:

The FBI supports DoDPI research through a cooperative agreement and currently has two SAs assigned to DODPI. Later this year, DoDPI will host a summit sponsored by the interagency Technical Support Working Group and DoD's Counterintelligence Field Activity. The purpose of assembling these experts is to develop a research plan for the next 5-10 years for means to assist in determining truth of statement.

49. In response to a previous question for the record regarding the New York Police Department (NYPD), you indicated that during a meeting to explore cooperation with the NYPD's translation and analysis program, the NYPD indicated that it did not want its officers and translation staff to undergo FBI polygraph testing as a condition of being granted access to "FBI information." The response further stated, "we understand that the CIA and Pentagon have found a means of ensuring trustworthiness without the use of polygraph examinations."

a. Please describe the alternative method of ensuring trustworthiness to which that response refers.

b. The previous response also stated, "We will work with both organizations to learn more about this process and will evaluate our ability to do the same." Please explain what progress has been made toward implementing this polygraph alternative.

Response to subparts a and b:

We have established a program where NYPD translators work on unclassified IC materials through the National Virtual Translation Center (NVTC). The FBI is also providing the NYPD with romanization training, teaching the IC's standard for transliterating foreign scripts into the Roman alphabet. Although we contacted our sister agencies to discuss their internal policies in this regard, we were pleased

to find the NVTC to be a suitable vehicle through which we could fully use the NYPD's available translator resources.

Questions Posed by Senator Kyl

50. I know that, for good reasons, you are not able to discuss operational details of the NSA's terrorist surveillance program. However, I was hoping that you could tell Committee whether, from your perspective, this program has made a significant contribution to your ability to prevent terrorist attacks against the United States homeland. Do you believe that the defunding or suspension of this program would make America more vulnerable to catastrophic terrorism?

Response:

The Terrorist Surveillance Program (TSP) has been valuable to the FBI in a number of terrorism investigations. We have received information from the TSP that has assisted the FBI in discovering individuals who are terrorists or are associated with terrorists. To the extent that suspension of this program could deprive our agents of this sort of information in the future, it would be cause for concern.

51. Alternative bills before the committee would require that the NSA surveillance program be briefed, in one proposal, to the Intelligence Committee alone and, in other proposal, to both the Intelligence and the Judiciary Committee. From your perspective as someone who is fighting terrorism on a daily basis, would it be desirable to keep both the full Intelligence and Judiciary Committees read into the program, or would it be better to restrict that access to the Intelligence Committee, which is accustomed to handling highly classified information on a routine basis?

Response:

Under Executive Order 12958, access to Special Access Programs (SAPs) is determined by the agency that creates the SAP. The FBI did not create the SAP referenced in the question and we would, therefore, defer to the NSA for response.

Questions Posed by Senator DeWine

52. Although there has been an increase in the overall number of agents at the FBI since 9/11, most, if not all, of those agents have gone directly to the Counterterrorism, Counterintelligence and Computer Intrusion Programs. In addition, between 9/11 and

FY06, there has been a reduction of 661 agents assigned to all Criminal Programs with another 300 slated to be eliminated by the President's Budget in FY07. This amounts to a reduction of between 10 and 15% of agents focusing on criminal matters. This has no doubt limited the number of criminal cases the Bureau has been able to investigate - - has it decreased effectiveness of the Bureau in fighting crime? How much of a priority is law enforcement? How have you compensated for the decrease in criminal agents?

Response:

The Funded Staffing Level for FBI criminal case agents has decreased by 994 agents, or 18%, since the attacks of 9/11. Despite the loss of those agent positions, protecting the nation's citizens from traditional criminal offenses has always remained a core function of the FBI, and 48% of all FBI agents remain allocated to these criminal matters.

To compensate for the decrease in criminal agents, the FBI has made difficult choices in determining how to most effectively use the available agents. In 2002, the FBI established as its criminal program priorities: public corruption, civil rights, transnational and national criminal enterprises (which include violent gangs and the MS-13 initiative), white collar crimes (which include corporate fraud and health care fraud), and violent crimes (which include crimes against children).

Since public corruption was designated as the top criminal priority, over 260 additional agents were shifted from other criminal duties to address corruption cases. The FBI is singularly situated to conduct these difficult investigations, and our effectiveness is demonstrated by the conviction of more than 1,000 corrupt government employees in the past two years.

The FBI has also maintained a steady commitment to addressing civil rights matters, and the number of these cases has remained fairly constant even as the complexity of the cases has increased. For example, the number of complex human trafficking cases has increased by almost 200% from 2001 to 2005, and the resolution of these cases has generally required both more time and more agents than the average non-human trafficking case.

The FBI has addressed violent street gang matters though its Violent Gang Safe Streets Task Force (VGSSTF) program, which leverages Federal, state, and local law enforcement resources to investigate violent gangs in urban and suburban communities. There are currently 128 VGSSTFs in 54 FBI field offices, composed of 561 FBI SAs, 76 other Federal agents, and 924 state/local law enforcement officers. The number of FBI SAs addressing gangs has increased,

with a decrease in the number of SAs addressing bank robberies, although the FBI still addresses violent and serial bank robberies.

Although the FBI has had to reduce the number of SAs working Governmental fraud matters since 9/11/01, FBI agents still respond to serious crime problems, as exemplified by the FBI's current initiatives to address hurricane-related fraud and Iraq contract fraud. The FBI does not currently open Governmental fraud cases unless the loss exceeds $1 million.

The FBI also prioritizes investigations within its White Collar Crime Program, emphasizing corporate/securities fraud and health care fraud. The corporate fraud cases, in particular, are very labor intensive, but they are a priority for the FBI because so many represent the private industry equivalent of public corruption, where the dishonest actions of a few people in leadership positions cause tremendous monetary losses and undermine investor confidence, both of which can threaten economic stability.

The FBI has also compensated for the decrease in SAs addressing traditional criminal matters by leveraging resources through the Organized Crime Drug Enforcement Task Force and High Intensity Drug Trafficking Area initiatives. In addition, the FBI has shifted criminal resources to implement the Child Prostitution and Violent Crime Task Force initiatives. The child prostitution initiative is a coordinated national effort to combat child prostitution through joint investigations and task forces that include FBI, state and local law enforcement, and juvenile probation agencies. This initiative has resulted in more than 500 child prostitution arrests (local and federal combined), 101 indictments, 67 convictions, and the identification, location, and/or recovery of 200 children. To address violent crime, the FBI has partnered with other state and local law enforcement agencies to create 24 Violent Crime Task Forces throughout the U.S. The FBI also funds and operates 18 Safe Trails Task Forces to address violent crime in Indian Country.

In addition to the above initiatives, the FBI has continuously worked to use technology, intelligence analysis, and enhanced response capability to leverage criminal program resources. In October 2005, the National Crime Information Center (NCIC) fugitive data base was integrated with the Department of State passport application system, resulting in automatic notification when fugitives apply for United States passports. In December 2005, eight Child Abduction Rapid Deployment Teams were established in four regions of the United States. These teams are available to augment field office resources during the crucial initial stages of a child abduction. The FBI is currently developing a means of integrating sex offender registries and other public data bases to better identify sex

offenders in the vicinities of child abductions and to "flag" sex offenders who have changed locations without satisfying registration requirements.

53. As you know, when individuals wish to naturalize and adjust their status, the US Citizenship and Immigration Services requests name checks from the FBI. We have had a number of cases in Ohio where the FBI backlog is creating very long delays which are harming the people who are requesting citizenship or waiting to have their names cleared for sensitive work. For example, my office has heard about long-term lawful permanent residents from Ohio who are applying to become U.S. citizens, and applied for name checks as far back as October of 2003, with no results yet. Some of these people are losing benefits that they would be entitled to, and which they rely on, if their names were cleared, yet they can't seem to get an answer from the FBI. Another Ohio resident will lose his job this week at Wright-Patterson AFB because his name check, submitted in August 2003, has not yet cleared.

Of course, it goes without saying that we need to take the time to make sure that applications for citizenship and clearances are thoroughly screened, but it is critically important that we do it in a timely way, both for security purposes and also to avoid the great hardships that these delays are imposing on many innocent and deserving applicants. I'm told that over a quarter-million cases have been pending for several years, which seems to be an unacceptably large backlog. What resources are being provided to address this problem, and when do you think the backlog will be cleared?

Response:

The FBI is sensitive to the impact of the delays in processing name check requests and is doing all it can to streamline the current, labor-intensive, manual process. Prior to 9/11/01, annual incoming workload averaged 2,500,000 name checks requests per year. The National Name Check Program (NNCP) is experiencing a post 9/11 spike in incoming work that peaked in 2003 at 6,309,346. The current workload averages 3,500,000 name checks per year. After 9/11, the FBI and United States Citizenship and Immigration Services (USCIS) agreed to enhanced search criteria and initiated a re-processing of 2,700,000 name checks. Of these, 15,088 remain pending final processing. Currently, the USCIS Name Check backlog is 302,016 name check requests.

Below is a summary of the initiatives the FBI is undertaking to address the backlog:

- The Name Check program is moving toward automating a primarily manual process by scanning paper files to provide machine-readable documents to build an Electronic Records System to allow for future automation of the process, which will reduce time spent locating files. At

this time, the FBI is scanning all paper files required for the Name Check process.

- The FBI is making enhancements to its Dissemination Database that will promote a paperless process within the next two or three months and provide a platform for commercial off-the-shelf products to greatly enhance search capability, improving tracking and workflow management.

- The FBI is collaborating with customer Agencies to enhance Name Check staffing by providing temporarily assigned employees and contractors to assist in the name check process.

- The FBI is in receipt of a custom Employee Training Program to significantly reduce new employee development time.

- The FBI is aggressively pursing ways to better customer relations. Name Check staff and USCIS staff interact on a daily basis regarding Name Check Issues. In March and April 2006, Name Check and USCIS staff jointly briefed Congressional staffers on name check and immigration issues.

- The FBI is pursuing a Fee Study to ascertain the cost of providing a name check to customer agencies. This will allow appropriate adjustment to fees charged thereby providing increased income needed to adequately resource the NNCP.

- The FBI is working with internal IT resources to improve search techniques with existing technology to increase quality of searches.

- RMD's NNCP is initiating technology upgrades in FY 2008 with a $4.2 million budget request.

- The RMD has initiated contracts to procure contractors to assist in processing name checks.

It is difficult to pinpoint a time when the backlog will be cleared because of the continuous incoming volume of name check requests versus the currently static limited resources of the NNCP. Additionally, the length of time a name check is pending depends on a number of factors that are case specific, such as the number of files an analyst must obtain (which is dictated by the number of "hits" on a name), the location and availability of those files, and the amount of information contained in a file that must be individually reviewed by an analyst. The steps

referenced above should allow the NNCP to accelerate its productivity in the near future allowing for a significant reduction on the backlog.

54. We have spoken before about the need for FBI Field Offices to have so-called SCIFs – Secure Compartmented Information Facilities -- where agents and prosecutors can examine classified information safely and securely. Obviously, this is a critical issue -- if we don't have enough space for our people to examine classified materials and enough classified computers and phone lines, we just can't fight terrorism effectively. In other words, if we don't have enough SCIF space, FBI agents will not be able to fight terrorism to the best of their ability. Despite the importance of this issue, I hear that many FBI field offices throughout the country still have inadequate SCIFs.

a. What, if any, plans does the FBI have to upgrade or expand its SCIF facilities?

b. What is delaying the deployment of adequate SCIF facilities?

c. What is your time-line for resolving the problems with SCIF facilities?

Response to subparts a-c:

SCIFs are being constructed on two tracks: (1) the first track includes those offices scheduled for standard renewal or relocations projects; (2) the second track includes those offices where new or expanded SCIFs are being constructed according to identified need, based primarily on a risk assessment.

In FY 2005, 5 Field Division offices, about 25 Resident Agencies, and 4 FBIHQ off-sites were undergoing standard renewal/relocation projects on the regular cycle, and some of these are still in the construction phase. As part of this cycle, 9 Field Division offices, 25 Resident Agencies, and 5 FBIHQ offsite projects are planned for each of the following years (FY 2006 and FY 2007).

Within the NSB, the Secure Work Environment Working Group has ranked the top 100 facilities for non-routine construction, based on a risk assessment. The FY 2006/2007 Secure Work Environment SCIF construction program will address these top 100 facilities (based on risk), in an effort to bring their capability in line with their mission.

The Secure Work Environment SCIF construction program is budgeted at $40,500,000 for FY 2006 (a $20 million enhancement on top of the $20.5 million dollar base). The President's budget for FY 2007 includes approximately $63,700,000 for SCIF construction ($30,500,000 in the base).

55. The FBI's computer system has been woefully ineffective and outdated for years, and it is critical that the new Sentinel computer system be implemented quickly and fully.

a. You mentioned in your written testimony that Sentinel will be rolled out over four years and in four phases. What are they, and what is the timeline for each phase?

Response:

Phase 1, scheduled for completion in April 2007, introduces the new Sentinel portal that provides access to legacy data, the case management workbox, and infrastructure components. The portal will initially provide access to legacy system data and will support future access to the new investigative case management system. The portal will employ web services technologies and provide users with browser access to investigative data without requiring them to understand the changes taking place in the system design. The first phase establishes a single point of entry for case management; improves the current web-based ACS capabilities by summarizing a user's workload on his dashboard, rather than requiring him to perform a series of queries to discover it. Furthermore, to simplify data entry into the FBI's Universal Index (UNI), a new entity extraction tool will identify persons, places, and things for automated indexing. Finally, core infrastructure components will be selected, and these may include an Enterprise Service Bus and foundation services.

Phase 2, scheduled for completion in May 2008, will begin the transition to paperless case records and electronic records management. Phase 2 will provide the information assurance and records management foundation upon which all future application services can be built. We will begin the replacement of legacy case management applications by integrating a commercial off-the-shelf database management system that will serve as the case document management repository, replacing the Electronic Case File portion of ACS. A workflow tool will support the flow of electronic case documents through the review and approval cycles. This phase will address the VCF Initial Operational Capability users' concerns that a paperless environment is necessary to obtain the benefits of automated workflow. A new security framework will be implemented to enhance system access authorization, role-based access controls, auditing, and Public Key Infrastructure-based electronic signatures.

During Phase 3, scheduled for completion in February 2009, the new global index database will replace UNI in ACS. The Sentinel global index will incorporate functional enhancements to overcome UNI's limitations. Sentinel will provide the ability to create and store index entries at both document and case levels, unlike UNI, which does not correlate index entries to documents. Sentinel index entry

types (i.e., persons, organizations, locations, incidents, property, and communication accounts) will support a wider range of attributes than currently offered by UNI. Furthermore, to improve the quality and completeness of index information, Sentinel will automate the extraction of index entries from the content of case documents. All index information within Sentinel will be searchable by leveraging the advanced searching capabilities that will have been integrated into Sentinel in Phase 2.

Phase 4, scheduled for completion in December 2009, will implement new case and task management and reporting capabilities and will begin the consolidation of case management systems. At the end of this phase, legacy systems will be shut down and the remaining cases in the Electronic Case File system will be migrated. Phase 4 will involve the replacement and consolidation of the following systems: Investigative Case Management, ASSET, Criminal Informant Management System, Financial Institution Fraud, Bank Robbery Statistical Application, Integrated Statistical Reporting Analysis Application, Case Document Access Report, and Guardian Threat Tracking System. Incremental changes to the portal and other services (e.g., searching) will be needed to accommodate new features being introduced.

b. Please elaborate as to what the FBI is doing to make sure that it is going to be done on time and at no more cost than what was contracted for?

Response:

Several measures have been initiated to tighten accountability in the execution of FBI contracts. Among other measures, all contracting officers will receive updated training with respect to the contract process that outlines current policy, regulatory changes, and new initiatives. In addition, the FBI's Finance Division has been reorganized to create a new unit responsible for coordinating acquisition planning, tracking, and reporting requirements for major programs. This unit will coordinate the development of an acquisition plan that clearly defines and documents the roles and responsibilities of key personnel, including the contracting officer, contracting officer's technical representative (COTR), program manager, property manager, and financial manager. These measures are designed to address the issues raised in the report by the GAO, including the need to establish clear lines of authority and accountability.

In the specific case of the Sentinel contract, the FBI has taken care to lay the groundwork for a successful major investment. The FBI has already implemented steps to ensure that all costs are authorized in advance, verified when products are delivered, and validated when invoiced. The Sentinel PMO includes both a dedicated contracting officer and a Business Management Unit (consisting of a

government business manager, budget analyst, Earned Value Management (EVM) analyst, cost estimator, and full-time COTR), which will track, monitor, and control all program and developmental costs.

Additionally, a separate, dedicated cost code for Sentinel has been established by the FBI's Chief Financial Officer (CFO) within the OCIO, allowing Sentinel, OCIO budget administration, and CFO teams to jointly track and control Sentinel costs through the Budgetary Evaluation and Analysis Reporting System and the oversight process. The FBI will augment this staff with audit support from the Finance Division to review invoicing and with the addition of an IV&V contractor, who will review the activities of the development contractor and the PMO to ensure the proper execution and delivery of the Sentinel system.

The FBI has conveyed to Sentinel's contractor, Lockheed Martin, the importance of detailed cost tracking and adherence to established policies and protocols based on the recent reviews by the GAO and the DOJ IG. Lockheed Martin understands our concerns and has assured us they will implement appropriate policies and procedures. Lockheed Martin's President and Chief Executive Officer, Robert Stevens, has stated that the Sentinel effort is one of his top six priorities. He will receive monthly updates on the status of the program from his leadership team. The President of Lockheed Martin Information Technology, Linda Gooden, stated during the 3/16/06 press event announcing award of the Sentinel contract: "Success is not an option; it is a mandate." The contract vehicle is structured so the contractor has clear reporting requirements, deliverables, and milestones. Although we do not anticipate Lockheed Martin will fall short in contract performance, the FBI has established managerial and contractual mechanisms to assess contractor performance throughout the process.

c. You have said that the contract can be terminated in whole or in part upon identification of poor performance. If that were to happen, what is the alternative? In other words, is termination a credible threat to maintain performance quality?

Response:

The FBI intends to succeed on this project and has dedicated considerable Program Management resources to ensure that any required corrective action is identified early enough to minimize poor performance. Nonetheless, the FBI is fully prepared to terminate the contract if warranted. We believe the termination of such a highly visible contract is a credible threat to a company such as Lockheed Martin.

d. You mentioned the Independent Validation and Verification of the monthly Earned Value Management Reports. Beyond that, to what extent will outside experts monitor the progress of the creation and implementation of Sentinel?

Response:

Several external agencies/groups will monitor or consult on Sentinel's development and implementation, including the following.

- Both GAO and the DOJ IG will audit the Sentinel program's developmental phase to assess the PMO's progress on Sentinel implementation.

- DOJ's Department Investment Review Board (DIRB) provides stewardship of DOJ's major IT investments and ensures they are aligned with the Department's mission and fiduciary obligations. The quarterly board is chaired by the DAG and vice-chaired by the DOJ CIO. That board has a disciplined agenda focused on program risks and risk management, budget and spending, and return on investment. After each program briefing, the board evaluates the program and "grades" the program's status. The DIRB also determines what areas require further review (action items).

  The Sentinel Program Manager presented the Sentinel Program to DOJ's DIRB in early January 2006, receiving conditional approval to continue the Sentinel program along with a few follow-up action items. The Program Manager responded to those issues, in writing, in mid-February 2006, and the DIRB gave the program "passing" marks. The Sentinel Program Manager formally addressed action items and the status of the program during the DIRB's presentation in early May 2006. At that time, the DIRB rated the program as "green" (acceptable) for program management readiness and "yellow" (moderate risk, needing periodic reviews) for the program itself. Although briefings are provided at the request of the board, the Program Manager has been briefing the DIRB on a quarterly basis and responding to any follow-on questions or required actions in a timely manner. We anticipate participating in future presentations to the DIRB.

- The FBI receives the volunteer assistance of several advisory groups comprised of well-regarded individuals from various private, corporate, and academic fields. For example, the Director's Advisory Board focuses at the strategic level, suggesting and assessing organizational strategies. This board meets quarterly and is chaired by Arthur Money, former Assistant Secretary of Defense for Command, Control, Communications,

and Information. Other members of this board include Lee H. Hamilton, Charles S. Robb, Richard L. Thornburgh, and James Q. Wilson. Other advisory boards include the CIO IT Advisory Council and the Markle Foundation. Sentinel also receives oversight from NAPA and the Surveys and Investigations Staff of the House Committee on Appropriations.

- Representatives of OMB, the ODNI, the DAG, and DOJ's CIO also meet periodically with the Sentinel Program Manager and senior managers in the FBI's OCIO and Finance Division for updates on various facets of the program.

Questions Posed by Senator Leahy

DOMESTIC SURVEILLANCE OF PEACE GROUPS

56. In February, the *Seattle Post-Intelligencer* reported that Federal Government antiterrorism agencies, including the FBI, conducted surveillance of local peace groups during recent Peace Fleet protests at Seattle's Seafair festival. Was the FBI involved in such surveillance and, if so, please explain the circumstances surrounding such surveillance.

Response:

The FBI did not participate in the surveillance of any local peace groups during Seattle's Seafair festival, which was the site of recent peace fleet protests.

57. At the hearing, we discussed the FBI's surveillance of the Thomas Merton Center (TMC), a Catholic peace organization in Pittsburgh. An FBI memo dated November 29, 2002, and titled "IT Matters" states that FBI agents photographed TMC leaflet distributors at a public anti-war event on November 29, 2002. You testified that the agents "were attempting to identify an individual who happened to be, we believed, in attendance at that rally." Please provide copies of *earlier* investigative memos that document the basis for the agents' belief that a person of interest in an International Terrorism Matter would be present during TMC leafleting activities on November 29, 2002.

Response:

The investigation of the individual whose presence at the rally was anticipated is still ongoing. Consequently, we are not able to discuss this investigation further. In addition, as noted in response to Question 59, below, these matters are pending review by DOJ's OIG.

58. Another FBI memo dated February 26, 2003, suggests that the FBI's surveillance of the Thomas Merton Center on November 29, 2002, was not an isolated incident. The memo, also titled "International Terrorism Matters," states that an investigation by the Pittsburgh Division Joint Terrorism Task Force (JTTF) revealed that TMC "has been determined to be an organization which is opposed to the United States' war with Iraq." The memo goes on to describe the anti-war messages on TMC's website, and also discusses anti-war protests that had taken place earlier in the month in Pittsburgh and across the country. When the FBI released this document in March 2006, it issued a Press Response stating that the memo "was actually a draft which was never finalized – nor made a part of an FBI file." That is heartening, but it is not a complete explanation.

a. What was the nature of the JTTF investigation documented in this memo?

b. How many investigators were involved?

c. Was the investigation approved by a supervisory agent?

d. What does it mean to say that the memo was never "made a part of an FBI file"? If it could be retrieved in response to a FOIA request regarding TMC, could it not also be retrieved for other purposes?

Response to subparts a-d:

In response to the FOIA request, the FBI conducted a manual search beyond its record system for all information responsive to the request. The 2/26/03 document was discovered during the search of a stenographer's computer hard drive for responsive information. This document identifies no author or file number and contains no markings indicating supervisory approval for entering into any FBI record keeping system. The Pittsburgh Division, where the document was located, was unable to identify the actual author or locate a file associated with this document. The document could possibly have been a draft that was never approved for filing. As a "loose" document, it could be retrieved only by someone with access to the computer on which it had been saved.

59. At the hearing, you said you would have the Inspector General look into this matter regarding the Thomas Merton Center. Have you referred this matter to the Inspector General and, if not, do you still intend to do so and when?

Response:

The FBI has referred this matter to the DOJ OIG and has been informed that the OIG will conduct a preliminary inquiry into the Thomas Merton Center issue to determine whether it is appropriate to formally open a case.

INTELLIGENCE VIOLATIONS

60. According to a recent report by the Office of the Inspector General, the FBI reported more than 100 possible intelligence violations to the President's Intelligence Oversight Board over the past two years. These violations included incidents where FBI agents intercepted communications outside of the scope of the order from the FISA court, and incidents where FBI agents continued investigative activities after their authority expired. What steps is the FBI taking to reduce the incidence of these types of intelligence violations?

Response:

The report by the IG referred to in this question included the results of the IG's examination of the FBI's process for reporting to the Intelligence Oversight Board (IOB) possible violations involving intelligence activities. The FBI takes all reports of possible IOB violations seriously and has a comprehensive process for conducting legal reviews of possible violations and referring them to the appropriate entities. Our internal process encourages the over-reporting of possible violations involving intelligence activities.

The IG has found no examples of willful disregard for the law or for court orders by the FBI. As the IG report notes, when possible violations are discovered, the FBI acts quickly to correct the error. In instances in which the violation involves over-collections or overruns involving the FBI's use of FISA authorities, the unauthorized collection is sealed and sequestered from the investigation. The possible violation is also then reported to the appropriate oversight entities.

Over the past four years, the FBI has realigned its investigative resources to balance the prevention of terrorism and foreign intelligence threats, but not at the cost of violating civil rights or civil liberties. FBI Special Agents are held to a very high standard in complying with the procedures currently in place to protect civil liberties and constitutional rights when using the legal tools appropriate for national security investigations.

TRILOGY AND SENTINEL

61. The Inspector General's March 2006 audit report on the FBI's planning for Sentinel identified several ongoing concerns about the project, including the FBI's ability to reprogram funds to pay for Sentinel without hurting other mission-critical operations. What steps are you taking to ensure that other critical FBI programs will not be hurt because of the $425 million price tag for Sentinel?

Response:

The FBI has determined that no reprogramming will be required for FY 2006 Sentinel operations. The funding requested in the President's FY 2007 budget will fund O&M for Phase 1 and most of the system development, training, and program management costs for Phase 2. If there are additional Phase 2 costs beyond the $100 million in the President's budget, the FBI will work with DOJ, OMB, and Congress to redirect existing funds where available or request additional funding as needed. Funding for Phases 3 and 4 and for the remainder of O&M for all Phases will be requested in future budget submissions. As noted in the response to the IG, the FBI evaluates the operational impact of any proposed reprogramming and takes that impact into consideration in all reprogramming decisions. The FBI routinely provides this impact assessment and other relevant information to DOJ, OMB, and Congress.

62. The Inspector General's report noted that, as of January 31, 2006, the FBI's Program Management Office (PMO) for Sentinel had only 51 of the planned full staffing level of 76 employees and contractors on board. The report cautioned that without full staffing during the first phase of the project, "the FBI runs the risk of not being able to oversee adequately Sentinel's aggressive delivery schedule." When do you expect to have fully staffed the PMO with qualified personnel?

Response:

The Sentinel PMO currently has funding for 77 positions, including 19 employees and 58 contractors. Currently, 58 of the 77 employees are on board (13 employees and 45 contractors). Six of the employees are on temporary duty or detail to the PMO from other offices.

The PMO had deferred hiring for some positions until the contract was awarded because filling those positions was unnecessary until that point. We are currently recruiting to fill five positions; those candidates will be selected within the next few months. The PMO will also begin active recruitment to fill an additional six positions (four employee and two contractor positions) within the next few months. The start dates for those in these six positions will vary depending on whether they are hired internally or externally, due to a number of factors including their security clearances and the time required for their background investigations.

Eight positions are currently vacant. Filling those positions has been deferred until we are closer to Phase 2 because they will support either O&M functions or Phase 2 development. We anticipate recruiting for these positions near the end of 2006.

63. The Inspector General's report expresses concern that although the FBI has considered its own internal needs when developing Sentinel's design requirements, it has not yet adequately examined Sentinel's ability to connect with external systems in other Justice Department components, the Department of Homeland Security, and other agencies. The report warns, "If such connectivity is not built into Sentinel's design, other agencies could be forced into costly and time-consuming modifications to their systems to allow information sharing with the Sentinel system." What steps is the FBI taking to prevent this scenario and ensure Sentinel's ability to share information with other intelligence and law enforcement agencies?

Response:

The Sentinel System Requirements Specification mandates the use of the open data exchange standards and protocols recently identified by DOJ for the exchange of law enforcement information and by other government agencies for the exchange of intelligence information. The Sentinel PMO has identified the legacy-supported law enforcement and intelligence systems with which Sentinel will interface initially and has developed the "as-is" (current) Interface Control Documents (ICD). The PMO will also analyze existing interfaces and develop the "to-be" (future) ICD necessary for additional information sharing. Sentinel is being developed to be compatible with the Extensible Markup Language (XML) standards used for data tagging and marking in both DOJ and the IC. The DOJ and IC standards will eventually merge to form the NIEM for metadata, with which Sentinel will also be compatible. The NIEM is managed by DOJ and DHS and is aligned with ODNI work. The NIEM will, therefore, provide a common standard for sharing information among law enforcement (Federal, state, tribal, and local), IC, and homeland security agencies.

As part of the Sentinel PMO's life-cycle management system, capacity for access by other law enforcement and IC agencies will be designed, assessed, reviewed, and approved as part of each Sentinel phase's preliminary design and design reviews. Sentinel's Test and Evaluation Master Plan calls for early interface testing to ensure compatibility and specifies interface monitoring and debugging tools to support verification and troubleshooting. The Sentinel PM provides monthly status briefings to OMB, ODNI, and DOJ on how these entities will use the national information sharing environment architecture, and there is additional close coordination with DHS regarding information sharing. Sentinel's PMO architects have also met with a number of other intelligence and law enforcement agencies through participation in Federal information sharing initiatives that include the NIEM, the Law Enforcement Information Sharing Program (LEISP), and the Law Enforcement Exchange Standard (LEXS). More than 30 government agencies participate in these initiatives and will conform to the information sharing specifications they establish.

The Sentinel PMO's work with outside agencies to improve information sharing capabilities includes the following.

- Sentinel architects have met on three occasions with DOJ's Chief Enterprise Architect to continue dialogs on the subjects of NIEM, the Global Justice XML Data Model (GJXDM), and LEISP. The FBI and DOJ are working together to harmonize information sharing initiatives and pursue a common interface to external systems.

- Sentinel architects have met with DOJ's Chief Data Architect to continue discussion of LEXS 2.0, particularly as it relates to the FBI's case file interface to our Regional Data Exchange (R-DEx) system. The R-DEx system is currently managed and maintained by the FBI's Office of IT Program Management, which also oversees the Sentinel Program. Further meetings are scheduled to examine revised interface requirements between R-DEx, the National Data Exchange (N-DEx), and Sentinel.

- Sentinel architects have worked extensively with DHS since the inception of the NIEM initiative. In addition, a representative of DHS Immigration and Customs Enforcement is now co-located with the Sentinel PMO and has attended Requirements Clarification Reviews with the Sentinel team.

- Sentinel architects have worked with ODNI's chief architect for more than two years. Meetings are scheduled to further discuss the NIEM initiative and the methods with which IC Metadata Working Group (ICMWG) artifacts are being harmonized with NIEM. The Sentinel architect has worked with the Terrorist Watchlist Person Data Exchange Standard (TWPDES) for almost two years and is familiar with the exchange standards envisioned by the TSC and the NCTC.

- Sentinel architects have reviewed the Common Information Sharing Standards (CISS) promulgated by the PM for the Information Sharing Environment (ISE), and much of the work needed to harmonize the FBI data model to these standards has already been done. The FBI will continue to work with Ambassador McNamara's staff and will move forward on their recommendations once the ISE PM"s Concept of Operations has been finalized. Extensive feedback on the Concept of Operations has been provided to the FBI's Office of IT Policy and Planning for incorporation into the overall FBI response on CISS.

The Sentinel PMO's approach to information sharing concentrates on the standardization efforts promulgated by other agencies within the Federal Government. Work on the technical committees and with PMOs for the NIEM,

GJXDM, TWPDES, ICMWG, ISE PM, ODNI OCIO, DOJ Enterprise Architecture Unit, and others gives the Sentinel PMO access to virtually every concerned government agency, with all of whom we share the common goal of sharing terrorism data in a near real-time environment. The Sentinel PMO will continue to interact and collaborate with all external system owners.

64. Inspector General Fine testified at the hearing that potential weaknesses in cost controls remain a continuing project risk for Sentinel. What are you doing to address this concern, so that the already high cost of the Sentinel program will not get out of control?

Response:

Please see the response to Question 55, above.

65. GAO's report on Sentinel's predecessor, Trilogy, found that weak controls on the part of the FBI and GSA resulted in the Bureau paying more than $10.1 million in unallowable costs and in the FBI being unable to account for more than 1,400 pieces of missing equipment, valued at approximately $8.6 million. The GAO report further noted that, given the scope of the oversight problems on the Trilogy project, there may be additional questionable costs not reflected in the its audit report. The GAO also recommended that you and the GSA Administrator take steps to investigate and recover these funds. Has the FBI taken any steps to recoup any of the at least $10.1 million in unallowable costs of Trilogy? If so, please state the amount of taxpayer funds that have been recovered by the FBI to date.

Response:

The GAO audit did not find or quantify unallowable costs, although weaknesses in internal controls did render the FBI vulnerable to paying potentially unallowable costs. GSA/FEDSIM is finalizing negotiations with GSA Deputy Assistant Inspector General (IG) for Auditing, FBI, and DCAA to have DCAA conduct an overall program audit of both task orders. The scope of the program audit will include the costs identified by GAO as potentially questionable. Upon completion of the program audit, DCAA will conduct the final closeout audit of both task orders. GSA/FEDSIM and the FBI will pursue reimbursement of any improper costs identified by that audit.

INFORMATION TECHNOLOGY

66. According to several recent press reports, some 2,000 employees of the FBI's New York Field Office will not all have access to e-mail accounts until the end of this year. The Assistant Director in charge of the New York Field Office has reportedly stated that the lack of email is a funding issue. How many FBI agents and analysts – in New York and

elsewhere -- currently operate without a government email account, and why? When do you expect that all FBI personnel will have email accounts?

Response:

Typically, FBI personnel access the Internet through either Law Enforcement Online (which is primarily used for law enforcement purposes) or the Unclassified Network (UNet) (which is a dedicated network that serves the FBI's operational and administrative needs, providing Internet connectivity and Blackberry service).

UNet was established in 2002 as the FBI's Internet Café (I-café). Similar to a public I-café, we anticipated that the UNet would be used in a kiosk environment where FBI employees would access the Internet at clustered locations. At its inception, the program was neither envisioned nor funded to provide individual users with desktop access.

In 2004, additional funding permitted the FBI to extend UNet access. To date, FBIHQ and 52 of the FBI's 56 Field Offices have UNet access, and some Field Offices also have locally arranged Internet access. A total of 24,365 UNet accounts have been assigned to FBI employees, task force members, and contractors. By the end of FY 2006, the UNet will be able to support 25,000 accounts and Internet access will be available on an additional 5,400 desktops. As additional funding becomes available, UNet will be further expanded to include the remaining FBI Field Offices and their Resident Agencies, with the ultimate goal of providing desktop UNet access for all FBI users.

Blackberry devices were first used in the FBI as a "continuity of operations" tool in advance of the Afghan conflict. There is, however, no dedicated funding for Blackberry purchase or use, and these devices are used by FBI Divisions on a limited fee-for-service basis. Expansion beyond this use is not possible without a substantial investment in both UNet and the Blackberry program.

INFORMATION SHARING

67. The GAO's most recent report on information-sharing found that more than four years after 9/11, we do not have government-wide policies and processes in place to improve the sharing of critical counter-terrorism information. What steps is the FBI undertaking to improve information-sharing with its Federal and local partners? What barriers do you see to effective information-sharing? What more can Congress do to help the Bureau improve its information-sharing capabilities?

Response:

The FBI has instituted several means of improving information sharing with our Federal, state, and local partners in the law enforcement and intelligence communities. Among these is the establishment of the FBI's Information Sharing Policy Board, which is chaired by the principal officer of the FBI for information sharing policy (currently the EAD, NSB). This board brings together the FBI entities that generate and disseminate law enforcement information and intelligence and is charged with implementing the FBI's goal of sharing by rule and withholding by exception. The FBI is also actively participating in the interagency effort to establish a terrorism ISE under the Presidential guidelines issued on 12/16/05.

The National Joint Terrorism Task Force (NJTTF), staffed with representatives from 38 Federal, state, and local agencies, enhances the coordination and cooperation among these government agencies. Through the NJTTF, the FBI provides a point of fusion for terrorism intelligence and supports the JTTFs, which are also comprised of personnel from the FBI and many other Federal, state, and local agencies and are located throughout the United States. Both NJTTF and JTTF members have access to FBI information systems.

Field Intelligence Groups (FIGs) are the FBI's primary interface for receiving and disseminating intelligence information, and a FIG has been established in each FBI field office. The FIGs, which complement the JTTFs and other task forces, are expected to play a major role in ensuring that the FBI shares what we know with others in the IC and with our Federal, state, local, and tribal law enforcement partners. FIGs participate in the increasing number of State Fusion Centers and Regional Intelligence Analysis Centers.

Within the law enforcement community, the FBI's National Information Sharing Strategy (NISS) is part of DOJ's LEISP and builds upon the capabilities offered by the FBI's Criminal Justice Information Services (CJIS) Division. The TSC, which was established to provide for the appropriate and lawful use of terrorist information to screen for known and suspected terrorists, also leverages the CJIS backbone to provide real-time actionable intelligence to appropriate Federal, state, and local law enforcement. Multiple Federal agencies participate in this effort, including the FBI, DOJ, DHS, DOS, and Department of the Treasury.

In the NCTC, analysts from the FBI, CIA, DHS, and DoD work side by side to identify and analyze threats to the U.S. and our interests. NCTC analysts produce the National Threat Bulletin, the Threat Matrix, and other analytic products. FBI SAs and analysts are also detailed to numerous other Federal entities, including the CIA, NSA, National Security Council, Department of Energy, Defense

Intelligence Agency, Defense Logistics Agency, and DoD's Regional Commands, adding yet another means through which information is shared with these organizations. The FBI also operates six highly specialized Regional Computer Forensic Laboratories designed to provide forensic examinations of digital evidence. In each of these laboratories, law enforcement agencies from all levels of government train, work, and share information.

Evolving technology offers ever greater ability to share classified information in secure environments. Within the IC, the FBI has a two-level approach. For those agencies that operate at the Top Secret/SCI level, the FBI is investing in the SCI Operational Network, a secure FBI network that is linked to the DoD Joint Worldwide Intelligence Communications System network used by the CIA, NSA, and other Federal agencies. The FBI also makes national intelligence more readily available to state, tribal, and local law enforcement agencies through the Law Enforcement Online network. Infrastructure threat information is provided to the private sector through the "sensitive but unclassified" InfraGard network.

For those agencies that operate at the Secret level, we have connected the FBI's internal electronic communications system to the Intelligence Community network (Intelink-S), which serves military, intelligence, diplomatic, and law enforcement users. As a result, FBI SAs and analysts who need to communicate at the Secret-level with other agencies can do so from their desktops.

The Law Enforcement N-DEx will provide a nationwide capability to exchange data derived from incident and event reports, including names, addresses, and non-specific crime characteristics. This information will be entered into a central repository available to law enforcement officials at all levels. The N-DEx is complemented by the R-DEx, through which the FBI is able to participate with Federal, state, tribal, and local law enforcement agencies in regional full-text information sharing systems under standard technical procedures and policy agreements.

68. The Office of the Inspector General recently released an audit report on the FBI's efforts to protect U.S. seaports from terrorism. The OIG review found that the FBI and the Coast Guard have not yet resolved issues regarding their overlapping responsibilities to handle a maritime terrorism incident. In his prepared hearing testimony, Inspector General Fine warned that, "a lack of jurisdictional clarity could hinder the FBI's and the Coast Guard's ability to coordinate an effective response to a terrorist threat or incident in the maritime domain."

a. In your view, what is preventing the FBI from reaching an accord with the Coast Guard regarding this crucial jurisdictional question?

b. Is legislative action needed to resolve this impasse?

Response to subparts a and b:

Please see the response to Question 19, above.

c. What do you think of the OIG's 18 recommendations for improving the FBI's counterterrorism efforts regarding seaport and maritime activities?

Response:

The FBI responded to the OIG report by letter from CTD Assistant Director Willie Hulon to IG Fine dated 3/17/06 (Enclosure A). That letter identifies the steps the FBI has taken and is taking in response to each of the findings and recommendations identified in the OIG report. The FBI is preparing a formal reply to the report that documents these and subsequent steps taken, and this process will be repeated every 90 days until the FBI has completed its response to all report findings and recommendations.

TERRORIST WATCHLIST

69. During the past year, the Terrorist Screening Center has initiated a record-by-record review of the terrorist screening database to ensure accuracy, completeness, and consistency of the records. Inspector General Fine has reported that the database currently contains more than 235,000 records and that TSC's review will take several years.

a. How can a list this large possibly be helpful to the FBI and its law enforcement partners in the effort to thwart terrorism?

Response:

The suggestion that the "large" size of the Terrorist Screening Database (TSDB) somehow makes it less helpful is incorrect. The size of the TSDB does not adversely affect the efforts of the FBI and its law enforcement partners to thwart terrorism. Rather, the TSDB - as maintained by the TSC - now serves to link the domestic law enforcement and intelligence communities, a link that did not exist before the attacks of 9/11/01. On 9/9/01, one of the 9/11 hijackers was pulled over for speeding by a law enforcement officer in Maryland. Since there was no consolidated watchlist to alert that officer that the individual he had encountered was a known terrorist, the officer did not have a chance to give that terrorist any extra scrutiny.

The June 2005 DOJ OIG Audit Report (Report 05-27) identified the need for a consolidated terrorist watchlist and, based on that recommendation, the TSDB was developed as the U.S. Government's consolidated database of all terrorist identity information based on nominations received from the FBI and the IC. If it comes to the attention of the TSC that an identity no longer exhibits a nexus to terrorism, that identity will be removed from the TSDB. The TSC engages in an ongoing effort to maintain the most thorough, accurate, and current information possible in the TSDB.

Practically speaking, the FBI and its law enforcement partners conduct electronic NCIC queries of the TSDB, so the size of the TSDB is not a factor. If a query results in a positive or possible match, the investigator is advised to contact the TSC; these calls are resolved in approximately five minutes. Unlike the officer who encountered the 9/11 hijacker on 9/9/01, law enforcement officers today who call the TSC receive a quick response advising them whether they are dealing with a known or appropriately suspected terrorist. Armed with that information, these officers are able to ask relevant questions, conduct consensual searches, and be alert to suspicious information or possible associates. Information obtained through these encounters is then fed back to the TSC and the IC for analysis, better enabling the U. S. Government to "connect the dots."

b. How much longer will it take for the TSC to complete its review?

c. What impact will the delay in getting an accurate terrorist watchlist have on the FBI's counterterrorism mission?

Response to subparts b-c:

As of 5/21/06, the Terrorist Screening Data Base (TSDB) contained over 491,000 records, but these records do not represent 491,000 separate individuals, since one individual may have multiple aliases or name variants or may claim multiple dates of birth, each of which is counted as a separate record.

The record-by-record review of existing TSDB records began on 4/1/05, but we cannot predict when this review will be completed because priority reviews of particular segments of information continually intervene. For example, while TSC formerly relied on the accuracy of information provided by agencies nominating individuals for inclusion in the TSDB, in March 2006 TSC began to conduct its own detailed review of each nomination to ensure all placements in the TSDB are appropriate. TSC data integrity analysts have also been asked to review the records of 4,000 frequently encountered individuals to ensure their inclusion on the No Fly list is appropriate, to review 1,383 domestic terrorist subject records to ensure the accuracy of handling codes, and to review records

marked in VGTOF as "silent hits." ("Silent hit" coding means the FBI case agent will be notified electronically of an encounter but the encountering official will not be aware of the "hit." This coding is used for several reasons, including when the subject does not pose a safety risk to local law enforcement and the investigation of the individual was opened based upon single source reporting or based upon classified information from a foreign law enforcement agency.) These high priority reviews are being conducted along with the daily average of 1,000 new nominations and requests for modification of existing records, all of which must also be rigorously reviewed and verified to avoid misidentification.

These reviews are being conducted in order to ensure that individuals who are included in the TSDB erroneously and do not pose a terrorism risk are deleted from the TSDB. Clearly, erroneous inclusion in the TSDB exerts a negative impact on the individual, such as when the person is prohibited by Customs officials from entering the United States or by the TSA from boarding a plane. While the recent review of the records of frequently encountered individuals should minimize such impacts, the FBI takes all errors seriously and is working to eliminate them. A complete record review will not, however, adversely affect our national security, because the errors this review is designed to detect are errors of excessive inclusion in the TSDB rather than omission from it. For this reason, the time required to complete this review will not impede the FBI's counterterrorism mission.

70. The Inspector General's June 2005 audit report on the Terrorist Screening Center found that its database designates nearly 32,000 "armed and dangerous" individuals at the lowest handling code, which does not require the encountering law enforcement officer to contact the TSC or any other law enforcement agency. Has anything been done to enable the TSC to designate individuals in such a way that law enforcement encountering them would be aware of the possible danger?

Response:

The premise of the question is faulty because it intermingles two separate databases that contain two different types of information. As discussed further below, the "armed and dangerous" designation is used in the NCIC database, while the "handling codes" to which the question refers are used in the VGTOF database. Consequently, it is not correct to say the TSC database "designates nearly 32,000 'armed and dangerous' individuals at the lowest handling code," because the "armed and dangerous" designation and "handling code" designations are not used in the same database.

When a law enforcement officer queries 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.

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 HSPD 6) 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.

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.

Additional information regarding the handling codes and related issues was provided to the Committee in response to Question 29 following the 7/27/05 hearing.

NATIONAL SECURITY LETTERS

71. The Justice Department has reported that in 2005, the FBI issued 9,245 national security letters for information on 3,501 U.S. citizens and legal residents. Let me repeat two questions I asked you at the hearing, which you were unable to answer at the time. (A) How do the 2005 numbers compare to the same numbers over the past 10 years. (B) Would you support declassifying those earlier numbers (for calendar years 1995 through 2004) and, if not, please explain why that information needs to remain classified when comparable and more current information is now publicly available.

Response:

During 2005, the number of National Security Letter (NSL) requests (excluding NSLs for subscriber information) for information concerning United States persons totaled 9,254 (versus 9,245 as set forth in the question). There were 3,501 different United States persons involved in these 9,254 NSLs.

Corresponding numbers are not available for the preceding 10-year period and it is not possible to retrieve them. These numbers were calculated for the first time in 2006 to report 2005 totals in satisfaction of the new reporting requirement enacted in the USA PATRIOT Improvement and Reauthorization Act of 2005 (3/9/06). To understand these numbers, please bear in mind the following points.

First, the above numbers reflect the FBI's good-faith effort to provide the most accurate information possible. However, because these numbers could not be compiled by computer, FBI personnel personally reviewed each 2005 NSL, confirming to the extent possible that any given United States person was not reported more than once. That effort was necessary because many names appear in the NSLs in a variety of forms or styles (e.g., John Doe and Johnny Doe; Elizabeth Roe, Liz Roe, and Betty Roe) and some individuals use one or more aliases. As a result, it is possible that, despite the best efforts of FBI personnel, the number of different United States persons reported above may include circumstances in which one person is reported multiple times.

Second, four statutes authorize the FBI's use of NSLs and the FBI has traditionally tracked NSL totals separately within each of those four categories. The FBI has not historically cross-referenced those four separate databases to distinguish different United States persons, in part because of the difficulties discussed above. This effort at cross referencing may also have resulted in errors.

Third, the FBI has not previously been required to distinguish between United States persons and non-United States persons when reporting NSLs involving financial institutions and consumer reporting agencies. While the FBI has compiled these numbers with as much accuracy as possible, this was accomplished by hand count and may include some inaccuracies.

Given the recent statutory requirement to compile and publicly report these numbers annually, the statistics sought by this question should be readily available for future years. It continues to be DOJ's position, though, that NSL numbers that were classified in previous years remain classified.

FBI EFFORTS TO SEARCH THE FILES OF JACK ANDERSON

72. In response to questions about the FBI's efforts to review the files of the late Jack Anderson, you stated that you were unfamiliar with the details of specific actions taken by the FBI.

a. Is it true, as was recounted by Senator Grassley, that FBI agents first approached Mr. Anderson's son, Kevin, and that he told the agents that he would discuss the request with his family before making a decision on whether to release documents?

Response:

The initial contact in this matter was a telephone call between FBI SAs and Mrs. Jack Anderson. The purpose of the call was to arrange a time for an interview. Mrs. Anderson's son, Kevin, subsequently contacted the SA who set up the interview to ask the reason for it and to request that his sister be present for the interview. Mr. Anderson advised that his sister was his father's caregiver in his later years and might be able to answer the FBI's questions. The evening after the first interview of Mrs. Anderson, an FBI Agent telephoned Mrs. Anderson for clarification of the ownership status of Jack Anderson's papers. Mrs. Anderson was unsure and directed the Agent to speak with her daughter. The Agent left a message for the daughter. When Mrs. Anderson's daughter failed to return the call, the Agent called Kevin Anderson, and he explained the ownership status of the papers.

b. Is it true that FBI agents then approached Mr. Anderson's widow and tried to "trick" her into signing a consent form that, in the words of Senator Grassley, "she did not understand"?

Response:

As indicated above, the FBI first spoke to Mrs. Anderson in the presence of her daughter and with knowledge of her son. After determining from Kevin Anderson that the Anderson family still owned the Jack Anderson papers, an FBI Agent called Mrs. Anderson and scheduled a second meeting at Mrs. Anderson's convenience. During this second meeting, Mrs. Anderson voluntarily signed three "Consent to Search" forms regarding the papers, for the three possible locations of the papers. The "Consent to Search" form is written in plain English, and Mrs. Anderson never indicated that she did not understand the forms or was uncomfortable in any way about signing them. It should also be noted that the FBI has not attempted to use the signed consents to gain access to the papers.

73. You testified that the FBI had recently c[o]me into possession of "information indicating that there may be classified national security documents within Mr. Anderson's collection." Is the FBI or the Department of Justice currently contemplating legal action to obtain access to the files of Mr. Anderson? If so, under what statutory authority would such an action be brought?

Response:

Based on information that there are classified documents within the Anderson papers, the FBI and DOJ are concerned that public access to such materials might cause damage to the national security of the United States. The FBI and the DOJ are assessing a variety of options but no legal action is currently contemplated.

Questions Posed by Senator Kennedy

I. Arab & Muslim Community

74. At the hearing, I asked you about the FBI's recruitment efforts in the Arab-American and Muslim communities. You indicated that there have been tangible results and that you could provide the Committee with figures. With as much specificity as possible, please tell the Committee what the results of these recruitment efforts have been. Please provide us with the figures that you mentioned in your testimony. In addition, please confirm how many new agents have been added since recruitment efforts began.

Response:

Since 09/11/01:

5,964 Applicants applied on-line for the SA position with a self-proclaimed fluency in a Middle Eastern Foreign Language.

506 SA applicants who speak a Middle Eastern Foreign Language had background investigations initiated.

162 SAs have been hired who have a Middle Eastern Foreign Language fluency.

The FBI has enhanced its recruitment initiatives for persons of Middle Eastern descent in myriad ways, including the following.

Recruitment Consultants

- *EdVenture Partners, Inc. (EVP).* EVP was tasked with developing partnerships and recruitment initiatives in Middle Eastern communities. These communities were an untapped resource for the recruitment of qualified applicants. The EVP contract has developed partnerships that will provide the FBI with a new vehicle to recruit qualified applicants on a national level as well as improve the FBI's relationships within the Middle Eastern community.

- *Recruitment Enhancement Services (RES).* In FY 2005, the FBI tasked this contractor to target applicants possessing critical foreign languages via "Internet mining" strategies. RES has been contracted by the FBI to utilize an innovative approach to recruit SA applicants fluent in critical foreign languages for which the FBI has a need. It is expected RES' innovative "Internet mining" techniques will greatly enhance the probability that applicants will successfully complete the FBI's processing and hiring procedures. RES received sufficient training pertaining to the needs of the FBI in late 2005 and developed their Internet strategy which is currently being implemented.

Advertisements

The FBI has conducted newspaper as well as television advertising on numerous Middle Eastern mediums, including, but not limited to: Afghan Community Television, Al Offok, Al Nahar, Bridges TV advertisement, Al Arabi, Al Hureya, Ultimate Media Inc., Detroit Chaldean Times, Al Akhbar, the Al-Sahafa newspaper, Arab World, Al Nashra, Al Manassah Weekly, the Arab Voice, Aramica, Al Arab Weekly, The Beirut, Arab American Business, Language Magazine, Arab American News, the Foreign Affairs Journal, Al Sahafa Newspaper, Dandana Arabic Television, Arab American Business Journal, the Arab American Chaldean Council, and the Middle Eastern Broadcasting Network of America.

Middle Eastern Partnerships

- *American Arab Anti-Discrimination Committee.* The FBI met with the American Arab Anti-Discrimination Committee regarding the recruitment of persons fluent in Middle Eastern languages. New ideas were discussed and added to the FBI's recruitment strategy targeting the Middle Eastern community and included: (1) utilization of monster.com's FAST TRACK to forward e-mails to targeted students and alumni meeting designated criteria; (2) requesting all Recruiters to identify Middle Eastern-oriented support groups on college campuses; (3) establishing a partnership with students on campus as well as internship programs; (4) identifying

organizations that employ students of Middle Eastern descent and invite them to tours of FBIHQ and Quantico; and (5) identifying on-board persons fluent in critical foreign languages or knowledgeable of Middle Eastern cultures to assist with recruiting.

- *United States Copts Association.* The FBI formed a partnership with the United States Copts Association whose membership consists of Egyptian Christians. This partnership was formed to network with the various churches and to advise the membership of the FBI's need for employees with Middle Eastern language abilities in the SA and other critical skilled positions such as Language Specialist and Contract Linguists. In November 2003, representatives from FBIHQ and the Los Angeles Division attended a dinner and a civic center event and discussed the FBI's need for Middle Eastern employees and employees with Middle Eastern language abilities.

Middle Eastern Student Programs

- *FBI Collegiate Marketing & Recruitment Program.* In FY 2002, the FBI entered into an agreement with EVP to initiate an education focused marketing approach to target students on diverse university campuses. This allows students, via a curriculum-based peer marketing strategy, to brand the FBI and market core occupation employment opportunities. This program has proven to be a great success.

- *Middle Eastern Foreign Language Honors Internship Program.* In 2005, the FBI developed a program to hire students as interns who possess fluency in a Middle Eastern language for the summer 2006 program. This program serves as an excellent feeder program to the SA position. Graduate and Senior level students are recruited to participate in this program. There were 16 students recruited for participation in this program and after language testing, 10 were selected to undergo the background investigation. Four students have successfully passed and will enter on duty 6/5/06 (one background investigation is still pending). This will be the first year for this program.

II. Hate Crime Statistics

75. You also testified that, "We keep statistics of hate crimes against Muslim-Americans, Sikh-Americans, Arab-Americans, and we can get you those." The FBI's report on Hate Crime Statistics, 2004 does not include specific information on Sikh-Americans and Arab-Americans. In light of reported and confirmed hate crimes against Arab and Middle Eastern communities since 9/11, why hasn't the FBI included a specific category in its

annual hate-crimes report that reflects the number of hate crimes targeting these communities? As I am sure that you are well aware, some Arab Americans are Christians so the existing category for anti-Muslim attacks is [i]nsufficient. Is the FBI willing to provide more information beyond "Anti-Other Ethnicity" to at least include "Anti-Arab Crimes?"

Response:

Pursuant to the Hate Crime Statistics Act of 1990, the FBI's CJIS Division, Uniform Crime Reporting (UCR) Program, collects and publishes information about hate crime incidents that have been investigated and voluntarily reported by more than 17,000 city, county, tribal, state, and federal law enforcement agencies across the nation. The Act, with its subsequent amendments, requires data be collected and published "about crimes that manifest evidence of prejudice based on race, religion, disability, sexual orientation, or ethnicity" and must not include "any information that may reveal the identity of an individual victim of a crime." The UCR Program complies with the OMB standards for federal statistics and administrative reporting with regard to Race and Ethnicity. As such, the FBI uses five categories for race (White, Black, American Indian/Alaskan Native, Asian/Pacific Islander, and Multiple Races) and two categories for ethnicity (Hispanic and Other Ethnicity/National Origin). The Anti-Arab category was originally included on the draft Hate Crime reporting form developed when collection of hate crime data began in 1990. After its review of the draft form, OMB disapproved the inclusion on the form of the Anti-Arab category pursuant to its approved information collection guidelines. CJIS discussed the possible inclusion of the Anti-Arab category with OMB again in approximately 2000, and in 2001. During this time span, OMB advised the previous information collection guidelines barring its inclusion remained in effect.

76. Would you also be willing to provide space for reporting more specific data on attacks against transgender individuals? Would you be willing to include information on gender-based crimes which is now collected by many states? If you are unwilling or unable to provide detailed statistics, can you please provide a detailed response explaining why you object to the inclusion of such statistics?

Response:

The Act does not authorize the collection of data about crimes motivated by a gender bias. Consequently, the UCR Program does not collect data about crimes motivated by gender bias.

77. In light of the increase in youth violence associated with gang activity across the country, I'm concerned that the FBI statistics do not contain specific information on the

nature and extent of juvenile involvement in hate violence - either as offenders or victims. Please provide this information.

Response:

The Act does not authorize the collection of data about the extent of juvenile involvement in hate violence. Consequently, UCR Program does not collect information about juvenile involvement in hate violence.

78. You also testified that a number of hate crimes have also been prosecuted at the State and local level. Can you confirm the number of federal hate crimes prosecutions in 2004, along with details relating to each case that you are including in the statistics?

Response:

The federal investigations that resulted in hate crimes prosecutions in 2004 were as follows:

Racial Discrimination involving force and/or violence:
11 Federal indictments and informations and eight convictions
7 local indictments/informations and 28 convictions

Racial Discrimination with no force or violence:
2 federal convictions
3 local indictments/informations and two convictions

Religious Discrimination involving force and/or violence:
1 federal indictment and conviction
5 local convictions

Religious Discrimination with no force or violence:
1 federal indictment

Housing Discrimination:
6 federal indictments/informations and 8 convictions
6 local convictions

Arab/Muslim/Sikh
During FY 2004, the FBI opened 77 Backlash Hate crime cases against Arab/Muslim/Sikh victims, resulting in 8 subjects being prosecuted federally and 13 subjects being charged locally.

III. Use of Confidential Informants:

79. As you know, a major scandal in the Boston FBI office led to important changes in FBI handling of confidential informants. Unchecked and unaccountable FBI agents in Boston failed to follow the Attorney General's Guidelines in handling such informants. These problems were not unique to Boston. A recent case in New York demonstrated that an FBI confidential informant, Greg Scarpa, was involved in several murders, yet the FBI did nothing. In fact, it was only last year that these murders were prosecuted – the District Attorney obtained the information from Congress, thirteen years after the FBI knew what had happened. In response to a question from Senator Cornyn, you also mentioned two other cases: 1) Fort Worth, Texas; and 2) the Leung Case in Los Angeles.

Can you please provide more detail on these three instances and describe whether the Attorney General Guidelines on confidential informants were followed in each of these cases? If not, can you please describe with specificity what steps were taken after the fact to address any failure to follow the guidelines? How have the protocols been changed? What new steps are taking place during FBI training to address these concerns?

Response:

The cases referenced above include the Leung Case in Los Angeles and the Scarpa case in New York. We believe the statement concerning a case in Fort Worth, Texas, was made by Senator Cornyn, rather than Director Mueller, and involves another law enforcement agency. The FBI would be happy to discuss with the Senator the case he was referencing.

The Leung case involved former FBI SSA James J. Smith, who became involved in an improper relationship with one of his informants. On one occasion, when Smith stepped out of eyesight, his informant, Katrina Leung, rifled through his belongings. This incident raised issues regarding the handling of human sources and contributed to the FBI's efforts to implement a comprehensive human source validation process to better detect the mishandling of sources.

The second case involved FBI informant Gregory Scarpa, Sr. and his FBI handler, retired SA R. Lindley DeVecchio. Scarpa testified in a number of major prosecutions against New York criminal organizations. It is alleged, however, that DeVecchio reciprocated by passing to Scarpa unauthorized information. This matter is currently before the court and a determination of DeVecchio's guilt or innocence has not yet been made.

While many of the FBI's confidential human sources have criminal histories or associations with known criminals, the information provided by these individuals is our most effective law enforcement tool. Since these incidents, the FBI has

undertaken several measures to minimize the inherent risks in using these sources. Among other things, the FBI has: provided to SAs at all levels training on source administration, operation, AG Guidelines, and internal FBI policies; required every division to assign a Human Source Coordinator to its FIG to monitor source files across all programs; mandated ongoing dialogue between FBI field offices and United States Attorneys' Offices to ensure SAs comply with legal requirements; and increased inspections of the Confidential Human Source Program Bureau-wide.

The Confidential Human Source Re-engineering Project is being designed to standardize policies and processes associated with managing and validating confidential human sources and to further improve compliance with AG Guidelines. We also anticipate that the IT systems we are developing to automate the handling of the administrative aspects of sources will significantly reduce, if not eliminate, compliance errors related to AG Guidelines. While no law enforcement agency can guarantee that its agents and sources will not engage in inappropriate conduct, misconduct by SAs operating sources does, fortunately, occur infrequently in the FBI. Violations of AG Guidelines and internal FBI policies are referred to the FBI's Inspection Division and OPR for investigation and adjudication.

80. As I mentioned at the hearing, last September, Inspector General Glen Fine reported that the FBI was not in compliance with the Attorney General's Guidelines in 87% of the FBI files examined. In nearly half of all the cases examined, the FBI did not comply with its obligation to notify state and local law enforcement about criminal activity by its confidential informants. Please describe, in detail what steps you have taken since the release of the Inspector General's report to ensure that past misuse of confidential informants will not happen again. What safeguards are in place to prevent abuses from occurring?

Response:

Although the OIG found the FBI 42% noncompliant with AG Guidelines regarding unauthorized activity by human sources, it is important to note that the OIG's finding concerned the FBI's obligation to notify either a United States Attorney or the head of a DOJ litigating component of criminal activity by its confidential informants (there is no requirement that the FBI notify state and local law enforcement). Recommendation 3 in the OIG report stated that the Bureau should "institute procedures to determine whether state or local prosecuting offices have filed charges against Confidential Informants who engage in unauthorized illegal activity to determine whether notification must be provided to the US Attorney's Office in accordance with Section IV.B.1.a of the Confidential Informant Guidelines." The FBI concurs that such procedures are desirable and

will explore how to best accomplish this goal, recognizing that a field office's ability to be informed of such matters may vary widely from jurisdiction to jurisdiction and recognizing, as well, that any such policy must be consistent with operational security and the protection of the source's identity. The current AG Guidelines and FBI policy require an SAC (or the equivalent) to notify an appropriate chief federal prosecutor immediately regarding a source's unauthorized illegal activity.

Determining whether a state or local prosecutor has filed charges against a source is the responsibility of the SA handling the source. Agents conduct periodic criminal record checks, maintain contact with their sources, and conduct ongoing background investigations of their sources to determine whether they have engaged in unauthorized illegal activity.

To enhance compliance with AG Guidelines, the FBI's DI has, in coordination with DOJ, initiated a comprehensive review and revision of our HUMINT program. During the past 2 years, the FBI has been developing new policies regarding the utilization of confidential human sources through our Confidential Human Source Re-engineering Project. The DI and DOJ are collaborating to simplify and standardize administrative procedures, clarify compliance requirements, and improve compliance with AG Guidelines. This re-engineering project will include the upcoming Confidential Human Source Validation Standards Manual and the subsequent implementation of a revamped validation process that will apply to all confidential human sources. SSAs, the FIGs, FBIHQ, and DOJ will all have roles in measuring the value of a source's operation as well as managing the risks associated with using a human source. Redundancy of review will be an intentional part of the validation process, serving as a check and balance on human source activities, including authorized and any possible unauthorized criminal activities. The EAD of the NSB has approved a draft of the Validation Manual, and the FBI is moving toward implementation throughout the FBI.

81. What measures are you implementing as a result of the Inspector General's report to improve information-sharing with state and local law enforcement?

Response:

The referenced report included a recommendation that the FBI institute procedures to determine whether state or local prosecuting offices have filed charges against confidential informants who engage in unauthorized illegal activity to determine whether notification must be provided to the U.S. Attorney's Office in accordance with the Confidential Informant Guidelines. The FBI concurred with the OIG's recommendation, noting the need to explore how best to

accomplish this goal while recognizing that a field office's ability to be informed of such matters may vary widely from jurisdiction to jurisdiction. In addition, new procedures must be consistent with operational security and the protection of source identity. These efforts are included in the ongoing comprehensive FBI/DOJ project to review and revise our Confidential Human Source program. The goals of that project are to develop new policies and processes for the utilization of confidential human sources that will simplify and standardize administrative procedures, clarify compliance requirements, and improve compliance with AG Guidelines. The FBI is also actively participating in the interagency effort to establish a terrorism ISE under the Presidential guidelines issued on 12/16/05.

Questions Posed by Senator Feinstein

82. As you offered at the hearing, please provide:

a. A description of how many of the 2,072 FISA warrants that the FBI obtained last year were "emergency" applications, as opposed to non-emergency applications.

Response:

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

b. The average amount of time the FBI needs to file and get a FISA warrant in each of these categories.

Response:

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

83. Do you ask people you appoint to top FBI counterterrorism and counterintelligence posts to commit in advance to stay there for an agreed-upon period of time? If not, why not?

Response:

Appointment to senior FBI positions are typically made following a conversation of commitment within the context of the work program plans and the personal circumstances of the individual.

84. At the hearing, I asked you about Inspector General Fine's report and its strong language relating to port security risks. You spoke of your plan to develop a new memorandum of understanding (MOU) with the Coast Guard to replace the draft MOU under which you have been operating for several years. I appreciate your stated concern "that we reach a more formalized understanding quickly." Can you please provide me a target date by which you expect to conclude this formalized understanding? And can you send me a copy of the FBI/Customs MOU once it is completed?

Response:

The interim MOTR Plan, which was approved by the President in October 2005, is currently being revised and we anticipate that the final plan will be approved by the President by late 2006. This final MOTR Plan will recommend protocols for each agency and will provide guidance for interagency coordination in response to maritime threats and incidents. After the final MOTR Plan is adopted, the FBI and USCG will address the need for an MOU, if any. The protocols established by the interim MOTR Plan and the pending final MOTR Plan have been used to guide responses to actual maritime incidents over the last several months, and the degree of interagency coordination and the speed with which joint decisions have been reached have been testaments to the effectiveness of these plans.

FBI Transition to a Domestic Intelligence Agency

85. As you are aware, depositions held last Summer reveal that top FBI counterterrorism and counterintelligence officials may have had limited experience in these fields beyond the on-the-job experience they obtained since 9/11. For example, the FBI's top counterterrorism and counterintelligence official, Gary M. Bald, was reportedly unable at his deposition to explain the difference between Sunni and Shia, and suggested that top FBI counterterrorism and counterintelligence officials don't necessarily even need such subject matter experience. In your view, how important is it that your top counterterrorism and counterintelligence officials understand the substance of Islam and Muslim cultures?

Response:

It is important that all investigators understand the dynamics that shape the terrorist threat facing our country. The FBI has made it a priority to ensure that our work force understands the bases of violent Islamic extremist ideologies, and has placed particular emphasis on understanding Muslim culture and the Islamic religion. This is evidenced by the counterterrorism and cultural training made available to our employees. This training teaches us to interact better with Muslim communities and to build the trust critical to effective community policing. Within the counterterrorism program, the provision to our counterterrorism workforce of the correct tools and relevant knowledge is one of

our highest priorities. CTD's current senior leaders have acquired this familiarity through their daily work, their past interactions with Muslim communities during field assignments, and study in this area. These leaders are also knowledgeable regarding terrorists' operational methods and their criminal activities, neither of which depend on Islamic ideology. Because management and leadership qualities are as important as substantive expertise, it is also important that CTD managers come to their jobs with lengthy and in-depth experience managing high-profile investigative and intelligence efforts.

Since 9/11, the FBI's counterterrorism program has grown quickly and is the FBI's top investigative priority. This rapid growth has been fueled by a reallocation of our best investigators, managers, and leaders to the counterterrorism mission. We have also refocused our recruiting and hiring to attract individuals with skills critical to our counterterrorism and intelligence missions. These new recruits have included hundreds of IAs, translators, and SAs.

86. John Gannon's written testimony describes the pre-9/11 world as one in which "[t]he terrorists knew more about our world, and how to train and operate in it, than we did about theirs – the classic recipe for an intelligence failure." Do we now know more about the terrorists' world than they do about ours? If not, is there a target date by which do you expect this goal to be accomplished?

Response:

The response to this inquiry is provided separately.

87. Please identify the number of linguists/translators that the FBI has hired in the last year – and in particular, how many of these new hires (quantified by language type) are fluent and/or proficient in the priority strategic foreign languages such as Arabic, Farsi, Chinese, etc.

Response:

The response to this inquiry is provided separately.

88. As one FBI official told the press, "If we become a terrific intelligence agency, we're one of 14 others," but "if we're the FBI, we're like none other." How does the FBI overcome this institutional barrier to elevating the importance of its domestic intelligence mission?

Response:

In any organization, there are those who will resist change and seek to maintain the status quo. Since 9/11/01, FBI employees have been faced with tremendous and continuing changes. These changes are being made quickly, but there are limits to how quickly such change can be made without adverse consequences, particularly while our employees continue to accomplish the FBI's important substantive work.

To achieve the integration of investigative and intelligence operations, the FBI established the DI to manage all FBI intelligence activities and resources. The DI leverages the core strengths of the law enforcement culture, with particular attention to the pedigree of sources and fact-based analysis, while ensuring no walls exist between collectors, analysts, and those who must act upon intelligence information.

The DI consists of a dedicated headquarters staff element and embedded elements in FBIHQ and field divisions. To oversee field intelligence operations, the FBI established FIGs in each of the 56 field offices. The FIGs are composed of SAs, IAs, and language analysts, and often include officers and analysts from other intelligence and law enforcement agencies. FIGs are central to the integration of the intelligence cycle (the six-step process of developing unrefined data into polished intelligence for the use of policymakers) into field operations.

To further develop our intelligence capabilities, the FBI has consolidated its national security investigative and intelligence missions under the NSB. As the next step in the FBI's evolution, the NSB combines the missions, capabilities, and resources of the counterterrorism, counterintelligence, and intelligence elements of the FBI. Building on the success of the DI, the NSB enhances the FBI's ability to meet current and emerging national security and criminal threats by integrating the FBI's intelligence mission more fully into the broader missions of the FBI and the IC. The NSB has full authority to manage all FBI intelligence activities, from collection to dissemination, and is vested with the authority to assign, prioritize, and reallocate intelligence resources.

Since our inception, the FBI has changed and evolved in response to new threats and expectations, and it was again faced with new challenges following the attacks of 9/11/01. Never before in the FBI's history has such a transformation been undertaken, particularly in such a short time. We have made enormous progress in building an intelligence capability, but further enhancements will take time. The FBI has established and is following a strategic plan for 2004-2009 that stresses the need for continuing change.

FBI executives emphasize these themes at every opportunity they have to communicate with employees, including through speeches, meetings, the FBI intranet, and e-mail messages. Nonetheless, experts in the transformation of organizations have indicated that, in any such transformation, 30% of the employees will support the change from the outset, 30% must be persuaded, and 30% will resist the change for a variety of reasons. The FBI must and will continue to win over those who are still on the fence and ensure that our employees recognize that the world has changed and that we must change with it.

FBI Terrorism Prosecutions

89. According to the Transactional Records Access Clearinghouse (TRAC), the FBI referred about 6,400 people for prosecution under anti-terrorism statutes in the first two years after the September 11 attacks. The Justice Department reported that it had obtained 184 terrorism convictions from the 6,400 cases developed mainly by the FBI. But according to TRAC, 171 of those convictions resulted either in no jail time or in sentences of less than one year – leaving only 13 with sentences of a year or more. Are these figures accurate? If not, how are they inaccurate?

Response:

DOJ's Executive Office for United States Attorneys (EOUSA) advises that the United States Attorneys' case management system shows that during Fiscal Years 2002 and 2003, the FBI referred 3,967 criminal matters against 4,779 suspects to the United States Attorneys. (It should be noted that referrals are made for investigation and are not necessarily recommendations for prosecution at the time the referral is made.) These criminal matters were classified by the United States Attorneys in the international terrorism, domestic terrorism, terrorism-related hoaxes, terrorist financing, and various anti-terrorism case categories. EOUSA is not certain how TRAC derived its number of FBI referrals.

The United States Attorneys' case management system also shows that during Fiscal Years 2002 and 2003, the United States Attorneys concluded the prosecution of 411 FBI-referred terrorism or anti-terrorism defendants. Of these defendants, 352, or 86 percent, were convicted. Of the 352 convicted defendants, 207 were sentenced to prison. Of the defendants sentenced to prison, 88 were sentenced to 1-12 months in prison, 48 were sentenced to 13-24 months in prison, 12 were sentenced to 25-36 months in prison, 29 were sentenced to 37-60 months in prison, 26 were sentenced to 61+ months in prison, and 4 were sentenced to life in prison.

The sentence imposed in a given case is not necessarily an accurate measure of the significance of the case in our counterterrorism efforts. Our strategy emphasizes

prevention, and a prevention strategy requires us to engage the enemy earlier than if we waited for them to act first. We cannot wait for terrorists to strike to begin investigations and make arrests. We must use the full range of criminal offenses at our disposal to charge offenses that fit the facts before those who would do us harm put their plans into action. Thus we use non-terrorism offenses, such as false statement charges, immigration fraud, and use of fraudulent travel documents, in terrorism cases. These offenses carry lesser penalties than offenses associated with completed terrorist acts, yet the appropriate charging of such offenses is so important to our disruption of terrorist plans that the Department has urged prosecutors to undertake initiatives to increase their use of these statutes. Defendants have also been sentenced to time served and immediately deported resulting in what would appear to be short sentences, but the result is that the defendant is removed from the United States.

In January 2003, the Government Accountability Office (GAO) issued a report entitled *JUSTICE DEPARTMENT: Better Management Oversight and Internal Controls Needed to Ensure Accuracy of Terrorism-Related Statistics*. This report summarized GAO's audit of Justice Department terrorism statistics. In the report, GAO stated that a review of EOUSA's Fiscal Year 2002 statistics on defendants convicted in terrorism cases showed that 132 of 288 cases were misclassified. Although GAO stated in the report that 127 of the 132 misclassified cases fell under newly established anti-terrorism program categories, GAO made recommendations for improving data integrity nonetheless. GAO recommended that in order to improve the accuracy and reliability of terrorism-related conviction statistics in Department of Justice's annual performance reports, a formal system should be implemented to oversee and validate the accuracy of case classification and conviction data entered in the United States Attorneys' case management system.

In August 2002, EOUSA issued new program category codes so the United States Attorneys could more accurately identify their terrorism and anti-terrorism cases. Prior to that time, the three terrorism-related codes were International Terrorism, Domestic Terrorism, and Terrorism-Related Hoaxes. New codes were added for Terrorism-Related Financing and for various Anti-Terrorism categories (such as Identity Theft, Immigration, and Violent Crime) to capture activity intended to prevent or disrupt potential or actual terrorist threats where the offense conduct would not fall within one of the already-existing codes. With a few exceptions, all the FY 2002 convictions that GAO identifies as "misclassified" were ultimately determined to be convictions properly classified in one of the Anti-Terrorism categories. With the transition to a new coding scheme so close to the end of the fiscal year, United States Attorneys' Offices (USAOs) either did not have time to, or did not fully understand the need to, reclassify already closed cases.

EOUSA complied with GAO's recommendation through the completion of formal Terrorism Case Data Quality Reviews by each USAO. All USAOs were required to update their information in the case management system, if necessary, and notify EOUSA that they had completed their review and update process by the deadlines set. EOUSA and the USAOs continue to monitor the accuracy of terrorism and anti-terrorism matter and case information in the case management system as part of the review and certification process that is conducted in each USAO in April and October of each year.

United States Attorneys code terrorism matters as International Terrorism Incidents Which Impact on the U.S., Domestic Terrorism, Terrorism Related Hoaxes, and Terrorist Financing. In addition, other matters are classified as Anti-Terrorism in the following categories: Anti-Terrorism/Environmental, Anti-Terrorism/Identity Theft, Anti-Terrorism/Immigration, Anti-Terrorism/OCDETF Drugs, Anti-Terrorism/Non-OCDETF Drugs, Anti-Terrorism/Violent Crimes, and Anti-Terrorism/All Others. The Criminal Division maintains its own statistics on terrorism cases which are very different from those maintained by the USAOs.

90. At an announcement with Attorney General Gonzales last Summer, President Bush stated that "federal terrorism investigations have resulted in charges against more than 400 suspects, and more than half of those charged have been convicted." But the Washington Post later reported that these numbers were "misleading at best" and that only "39 people – not 200, as officials have implied – were convicted of crimes related to terrorism or national security." And a January 2003 GAO report stated that the Justice Department "does not have sufficient management oversight and internal control standards to ensure the accuracy and reliability of its terrorism-related statistics." In your view, how many federal criminal cases that truly involve terrorism or national security, and that have yielded convictions and prison sentences in excess of one year, have been brought by the FBI since September 11, 2001?

Response:

DOJ's EOUSA advises that the numbers quoted by the President are based on statistics that represent defendants charged in terrorism or terrorism-related criminal cases with an international nexus that are tracked by DOJ's Criminal Division. The Criminal Division maintains its own statistics on terrorism cases which are based on different criteria from those maintained by the USAOs.

Cases tracked by the Criminal Division arose from investigations primarily conducted after 9/11/01, which initially appeared to have an international connection, including certain investigations conducted by the FBI's Joint Terrorism Task Forces (JTTFs) and other cases involving individuals associated with international terrorists or Foreign Terrorist Organizations. The Criminal

Division began tracking these cases during the nationwide PENTTBOM investigation of the 9/11/01 attacks; indeed, the initial cases tracked involved individuals identified and detained in the course of that investigation and subsequently charged with a criminal offense, though often not a key terrorism offense. Additional individuals have been added who, at the time of charging, appeared to have a connection to terrorism, even if they were not charged with a terrorism offense.

The Criminal Division also keeps track of all material support, terrorism financing and related cases. The material support statutes are the cornerstone of our prosecution efforts. The Criminal Division tracks a subset of cases that are reported through the case management system of the USAOs. For purposes of the USAO system, "Terrorism" investigations and cases include International Terrorism, Domestic Terrorism, Terrorist Financing, and Terrorism-Related Hoaxes; and "Anti-Terrorism" investigations and cases include Immigration, Identity Theft, OCDETF, Environmental, and Violent Crime - all in cases where the defendant is reasonably linked to terrorist activity or where the case results from activity intended to prevent or disrupt potential or actual terrorist threats.

Applicable criteria used by the Criminal Division as to which cases it tracks includes: whether a terrorism statute is charged, whether it derives from a JTTF investigation, whether the conduct involves a terrorist act or terrorist activity, whether the individual charged is associated with terrorists, a designated foreign terrorist organization, another terrorist group, or a Specially Designated Terrorist.

Proactive prosecution of terrorism-related targets on less serious charges is often an effective method of deterring and disrupting potential terrorist planning and support activities. Moreover, pleas to these less serious charges often result in defendants who cooperate and provide information to the Government - information that can lead to the detection of other terrorism-related activity.

Based on statistics maintained by the Criminal Division of terrorism and terrorism-related criminal cases with an international nexus, as of 6/22/06: 441 defendants have been charged,[1] resulting in 261 convictions in 45 jurisdictions,[2] including 218 guilty pleas, 43 convictions after trial, 150 cases remain pending,[3]

---

[1] This includes three defendants, each of whom was charged in two separate indictments; each indictment is counted as a separate case, so these three defendants are counted twice.

[2] Two of the defendants are counted twice here, reflecting that each was charged and convicted in two separate indictments. A third defendant has been convicted in one case and has another case pending against him.

[3] Pending cases include those in which the defendant is in pre-trial detention awaiting trial, or the defendant is a fugitive or is awaiting extradition; this also includes a number of cases under seal.

29 cases which have not resulted in conviction and are no longer pending,[4] and 1 case which resulted in mistrial and is awaiting re-trial on the same charges.

The Criminal Division does not keep comprehensive sentencing data on all terrorism cases. The sentence imposed in a given case is not necessarily an accurate measure of the significance of the case in our counterterrorism efforts. Our strategy emphasizes prevention, and a prevention strategy requires us to engage the enemy earlier than if we waited for them to act first. Again, we cannot wait for terrorists to strike to begin investigations and make arrests. We must use the full range of criminal offenses at our disposal to charge offenses that fit the facts before those who would do us harm put their plans into action. Thus we use non-terrorism offenses, such as false statement charges, immigration fraud, and use of fraudulent travel documents, in terrorism cases. These offenses carry lesser penalties than offenses associated with completed terrorist acts, yet the appropriate charging of such offenses is so important to our disruption of terrorist plans that the Department has urged prosecutors to undertake initiatives to increase their use of these statutes. Defendants have also been sentenced to time served and immediately deported resulting in what would appear to be short sentences, but the result is that the defendant is removed from the United States.

Effect of FBI Transition on its Traditional Law Enforcement

91. The FBI's primary focus after 9/11 must be on stopping terrorism, and the FBI has formally reallocated 1,143 agents to terrorism-related programs. But according to Inspector General Fine, the FBI in FY2004 was utilizing almost 2,200 fewer field agents to investigate its more traditional crime matters than in FY2000. During that same time, the FBI opened 28,331 fewer criminal cases (a 45% reduction), and reduced the number of matters referred to U.S. Attorneys for prosecution by 6,151 (27%). Inspector General Fine noted that, for some specific crime areas, such as financial institution fraud, there is now "an investigative gap." We are also hearing of how FBI surveillance squads are increasingly being used for counterterrorism instead of traditional law enforcement surveillance, in areas such as organized crime. Is this drop-off likely to be the FBI's new norm? Would additional resources substantially increase the number of FBI arrests and referrals for prosecution in these traditional areas?

---

[4]Among the 29 charged cases that did not result in a criminal conviction and are no longer pending, 4 defendants were transferred to Customs and Immigration Enforcement (ICE) custody for removal or deportation; 8 were indicted on or have pled guilty to other charges; 8 were dismissed on the government's motion for evidentiary or other reasons; 1 died while still a fugitive; and 1 had his charges dropped after he was designated an enemy combatant by the President.

Response:

The FBI has a broad mission with varied and competing challenges. In order to discipline the FBI's approach to these challenges, we have considered the interaction of three factors: (1) the significance of the threat to the security of the United States as expressed by the President in National Security Presidential Decision Directive 26; (2) the priority the American public places on various threats; and (3) the degree to which addressing the threat falls most exclusively within the FBI's jurisdiction. Weighing and evaluating these factors resulted in the FBI's top ten priorities. The first eight are listed in order of priority. The final points (collaborative partnerships and technology improvement) are key enabling functions that are of such importance they merit inclusion. The priorities are:

1. Protect the United States from terrorist attack;
2. Protect the United States against foreign intelligence operations and espionage;
3. Protect the United States against cyber-based attacks and high-technology crimes;
4. Combat public corruption at all levels;
5. Protect civil rights;
6. Combat transnational and national criminal organizations and enterprises;
7. Combat major white collar crime;
8. Combat significant violent crime;
9. Support federal, state, local, and international partners;
10. Upgrade technology to successfully perform the FBI's mission.

The FBI staffs and works high priority matters before lower ones. Support processes, including hiring and technological competence, serve our highest priorities first and resources are allocated and applied to each FBI mission according to its priority. The counterterrorism effort has received significant financial and human capital resources since 9/11/01; those resources have been used to build our capabilities and to re-engineer the FBI into a proactive, intelligence-gathering organization committed to protecting the United States from future terrorist attacks.

While our national security efforts remain our top priority, the FBI continues to fulfill our crime-fighting responsibilities as well. As the Committee was informed by the Director in his opening statement, public corruption is the top criminal priority for the FBI. Over the last two years, the FBI's investigations have led to the conviction of over 1,000 government employees involved in corrupt activities, including 177 Federal officials, 158 state officials, 360 local officials, and more than 365 police officers. Among its other priorities, the FBI also continues to focus on implementing the National Gang Strategy, along with ATF. This strategy is designed to identify the prolific and violent gangs in the United States

and to aggressively investigate, disrupt, and dismantle their criminal enterprises through prosecution under appropriate laws.

As always, the FBI will work with DOJ, OMB, and the Congress to determine whether to seek additional resources in support of the FBI's numerous responsibilities.

92. I understand that the President's budget from OMB for FY2007 recommends only one new agent to be added to the overall staffing total for the entire FBI, nationwide. Do you believe that the FBI, on this proposed budget, can continue to perform its expanding responsibilities in the areas of counterterrorism and counterintelligence, while still adequately maintaining its traditional law enforcement capabilities?

Response:

For the FBI to perform its law enforcement and national security responsibilities it requires both qualified personnel to fill agent, analyst, and other support positions, and infrastructure, including IT systems and SCIFs. In each year since FY 2002, the FBI has received funding from Congress to bolster its infrastructure and to hire thousands of new positions (1,681 SA and 4,347 support positions from FY 2003 through FY 2006). However, even with infrastructure successes like IDW and other IT systems, the FBI's infrastructure has not kept pace. The FY 2007 budget was formulated with this in mind and it focuses on providing the infrastructure and tools necessary for agents and analysts to do their jobs, from $100 million to move the Sentinel project forward to $64 million to build new SCIFs across the country. While additional personnel may be necessary in the future, the FY 2007 budget provides the infrastructure resources necessary for current FBI personnel to be more effective and efficient in their jobs.

93. I understand that thought has been given to using the "intelligence" model more broadly within the FBI, allowing cases to be opened and investigations begun without the predicate of suspicion of a crime. While this may be a necessary step to prevent major crimes such as terrorism, there are profound implications for the nation's leading law enforcement body to be investigating Americans who are not, at the time, in violation of the law. What is your view on the necessity to open preliminary investigations to identify the potential intent to commit crimes, and the ways in which such investigations can be safeguarded against intruding on civil liberties?

Response:

The FBI does not open either preliminary or full investigations without predication. To fulfill its mission, though, the FBI is responsible for identifying threats that are not readily observable. To do this, we have required our field

offices to learn about their territories using domain management, which gives field offices a top-down understanding of their territories that complements the intelligence derived from cases. The field offices use these assessments to identify and prioritize threats and to make better-informed decisions about where to focus resources to most effectively disrupt those threats. This learning process is nonintrusive. FBI offices learn from confidential human sources, local officials, concerned citizens, and businesses. If a field office learns of a potential national security threat (for example, if a source indicates the presence of a terrorist cell), that field office may open a threat assessment to determine the validity of the threat. Threat assessments are conducted using nonintrusive techniques that are generally different from domain management only in the sense that the assessment is focused on the possibility of an identified threat. The threat assessment is designed precisely to gain information about a focused issue without intruding on civil liberties. If a threat assessment validates a potential threat, then a predicated investigation may be opened.

We are aware that we cannot be effective in either our criminal mission or our intelligence mission without the support of the public. If the FBI were to investigate Americans without predication, we would quickly lose the confidence of the public, which is a significant source of the information we need to accomplish our missions.

Information Technology Concerns: "Virtual Case File" and "Sentinel" Systems

94. According to the Inspector General's March 2006 Audit Report 06-14, the FBI had not disclosed its specific cost estimates for Sentinel because the contract had not yet been awarded, but "[a]ccording to the FBI, a more precise cost estimate will be available once the FBI awards the Sentinel contract. . . . ." Now that the Sentinel contract has been awarded, what are the FBI's specific cost estimates for the Sentinel project?

Response:

As indicated in response to Question 13, above, the total value of the contract with Lockheed Martin is $305 million over 6 years, including both development and O&M. The FBI estimates that the total cost of the Sentinel program, including program management, systems development, O&M, and IV&V, will be $425 million over 6 years.

95. According to that same audit, the Sentinel acquisition plan identified seven risk factors, including concerns about scope creep and that initial program costs may be underestimated. The audit also noted that the Program Management Office has not yet been fully staffed, that "it is critical for the FBI to fully staff the PMO office as soon as possible" and "for the PMO to have stable leadership," and that "[w]ithout a fully staffed,

stable and capable PMO managing the project on a daily basis, Sentinel is at risk." Both this IG audit and the GAO's Linda Calbom identify weaknesses in FBI cost control, and warn that the FBI will be "highly exposed to the same types of negative outcomes that they experience with Trilogy" unless these weaknesses are corrected. Please explain how the FBI has addressed or is addressing these concerns.

Response:

Please see the responses to subparts a and d of Question 55, above, regarding cost control issues. The FBI has strengthened its internal controls and contract oversight in several ways in order to avoid a repetition of prior problems.

- First, the Sentinel contract has clear reporting requirements and defined deliverables in each contract phase (each of the four phases delivers capability to the end-user), and the contract can be terminated at any point should these results be unsatisfactory.

- Second, those responsible for contract management have clearly defined roles and responsibilities, and the management function is structured so as to ensure that accountable personnel review all documentation and expenses. The FBI has implemented measures to verify the FBI's receipt of deliverables and to validate their costs when invoiced. This contract management function will be supplemented by internal financial management audits.

- Third, an IV&V specialist will report directly to the FBI's CIO and will independently assess the efficiency and progress of the PMO and the work of the Sentinel contractors.

- Fourth, to eliminate the likelihood of "scope creep," any significant requirement changes must first be approved by the FBI's Deputy Director.

Please see the response to Question 62, above, regarding the PMO's staffing.

96. According to the Inspector General's March 2006 audit, the FBI plans to reprogram funds to pay for the first two phases of Sentinel. Congress approved the first phase ($97 million in reprogramming of FY2005 funds) in November, with more than $27 million of this reprogramming coming from Counterterrorism and intelligence-related activities. While the audit noted that the FBI's divisions and offices had reported an ability to absorb this first diversion of funds to Sentinel, they also reported that "a second reprogramming of the same magnitude would damage their ability to fulfill their mission." The auditors also noted concern "that diverting substantial funds from such mission-critical areas could begin eroding the FBI's operational effectiveness." Does the FBI plan to seek a second

phase of reprogramming of funds to pay for Sentinel? Given that we are already hearing anecdotal stories about FBI field offices placing monthly caps on agents' gasoline expenditures, how can it do this without compromising its operational effectiveness?

Response:

Please see the response to Question 61, above.

97. The Inspector General also noted concerns "that the FBI has not yet adequately examined or discussed Sentinel's ability to connect with external systems in other [DOJ] components, the [DHS], and other intelligence community agencies. If such connectivity is not built into Sentinel's design, other agencies could be forced into costly and time-consuming modifications to their systems to allow information sharing with the Sentinel system." For example, the DEA's Deputy CIO already reported in that same audit how its new case management system "is not compatible with Sentinel as currently designed." Once Sentinel is implemented, do you anticipate that Congress will face substantial additional costs in the future based on a need to implement interoperability between the various intelligence and law enforcement agencies' systems?

Response:

Please see the response to Question 63, above.

98. On a practical level, once Sentinel is fully implemented, and a local cop makes a traffic stop of the next Mohammed Atta (i.e., a terrorist whose name and identifiers are on the FBI's terrorist watchlist), will the local cop or a local police station be able to perform a Google-like electronic search to find that out? If not, why not, and what more will it take to get to that place?

Response:

The FBI intends for Sentinel to interface with the N-DEx system. With this interface, local law enforcement with access to N-DEx will be able to perform searches on Sentinel data exchanged with N-DEx.

FBI Activities at Pomona College, California

99. I have been contacted by several constituents concerning an FBI informational interview of Professor Tinker Salas, a professor of Latin American history at Pomona College in California. Can you please provide me with a description of the circumstances surrounding this interview, and whether you believe the agents' actions were appropriate?

Response:

Although the FBI is not at liberty to disclose information pertaining to FBI investigations, the interview of Professor Tinker-Salas was conducted for reasons unrelated to his position as an academic professor. As a general matter, the FBI conducts interviews to gather information that is pertinent to our responsibilities to protect the national security. Overt interviews, in which FBI agents identify themselves and the interviewee is free to decline to speak, are frequently used to gather basic information from people who wish to cooperate with the FBI. In this case, it is worth noting that Dr. Tinker-Salas is a noted historian with a deep understanding of Venezuelan politics, culture and history. The FBI did not intend to, nor did it, violate Dr. Tinker-Salas' First Amendment rights.

NSA Surveillance Program

100. Has the FBI received, via information sharing, information from the NSA's domestic wiretapping conducted outside of FISA? If so, is a system in place, either at the FBI or NSA, to identify when information was obtained without a FISA warrant? Does the FBI have any minimization procedures in place for information shared with the FBI by the NSA that has been obtained outside of existing FISA procedures? If so, please describe those procedures and the date when they were enacted.

Response:

It is not appropriate to discuss the operational details of the Terrorist Surveillance Program in this context. The full Senate Select Committee on Intelligence has been fully briefed on the operational details of the TSP described by the President.

101. Has the FBI, like the NSA, conducted non-Title III domestic electronic surveillance (hereinafter "domestic wiretapping") without obtaining or seeking a FISA warrant? If not, why has the FBI chosen not to do what the NSA has done? If so, please describe (in a classified submission, if necessary) the nature of the FBI's activities, the date on which such domestic wiretapping without FISA court approval began, and the reason(s) why the FBI determined that FISA warrants were not legally required for these activities.

Response:

All electronic surveillance conducted by the FBI is in accordance with the Constitution and laws of the United States. The FBI conducts domestic electronic surveillance pursuant to Title III and FISA. In addition, the FBI engages in two types of surveillance without court order: consensual monitoring (based on the consent of one party to the conversation) and under circumstances in which there is no reasonable expectation of privacy. The TSP is not a "domestic" surveillance

program. Rather, that program targets for interception only international communications where NSA determines there is probable cause to believe that at least one party to the communication is a member or agent of al-Qa'ida or an affiliated terrorist organization.

102. In his written testimony, Inspector General Fine noted how the FBI has reported a variety of claims of civil rights and civil liberties violations to the President's Intelligence Oversight Board ("IOB"), including some in FYs 2004 and 2005 relating to "intercepting communications outside the scope of the order from the FISA court," and how "[n]ot all possible violations were attributable solely to FBI conduct." Did the FBI ever submit, to the IOB, concerns about the NSA's (or the FBI's, or any other agency's) activities relating to domestic wiretapping without a FISA warrant? If so, please provide the date and subject matter of such submissions, and please produce all such submissions that the FBI sent to the IOB (in classified form, if necessary).

Response:

The FBI's obligation is to report intelligence activities affecting FBI investigations that violate law, AG Guidelines, or the FBI's internal policies established to protect the rights of United States persons. Because DOJ has opined that the TSP is lawful, there has been no basis for reporting activities related to that Program to the Intelligence Oversight Board.

Questions Posed by Senator Feingold

National Security Letters

103. When you appeared before the Judiciary Committee on May 2, 2006, I asked you about the disparity between the number of National Security Letters (NSLs) that were issued in 2005 versus the number of Section 215 business records orders issued in 2005. You agreed that obtaining a Section 215 order requires judicial approval, and that issuing a NSL does not require judicial approval, but said that you would get back to me about why so many more NSLs were issued in 2005. Please provide a response.

Response:

NSLs are available to obtain the records that form the basic building blocks of most investigations (e.g., telephone records and banking records). They are used frequently and in many national security investigations (similar to the role of grand jury subpoenas in criminal investigations). Orders pursuant to Section 215 of the USA PATRIOT Act, on the other hand, are used only if the records cannot be obtained through other means (e.g., through NSL or voluntary production).

The preference toward NSLs is not borne of any desire to avoid judicial review, but rather from a desire to obtain the information needed to pursue a national security investigation in the most efficient way possible under the law. Because NSLs can be issued at the field office level, they are far more efficient than 215 orders, which require court filings.

NSA Wiretapping Program

104. When did you first learn about the NSA wiretapping program authorized by the President shortly after September 11, which circumvented the FISA court process?

Response:

Director Mueller became aware of NSA's TSP at or near the time the program commenced.

105. Did you raise any objection to the NSA wiretapping program at the time?

Response:

As I explained at the hearing, I do not believe I should go into internal discussions I may have had with others in the Executive Branch.

106. Do you have any concern that judges would not permit the information gathered through the use of these wiretaps to be used in criminal prosecutions?

Response:

The purpose of the TSP is to gather intelligence about what al-Qa'ida and affiliated terrorist organizations are planning, particularly in the United States or against United States interests, not to gather evidence for use in criminal proceedings. The FBI has used FISA and Title III as the exclusive means of eavesdropping on individuals within the United States, whether we are attempting to develop evidence for use in criminal proceedings or to gather foreign intelligence.

107. Has anyone in the Administration, either at the White House or the Justice Department, urged you to use information derived from this wiretapping program in a criminal case?

Response:

The purpose of the TSP is to gather intelligence about what al-Qa'ida and affiliated terrorist organizations are planning, particularly in the United States or against United States interests, not to gather evidence for use in criminal proceedings. No one in the Administration has urged the FBI to use information obtained through the TSP in a criminal case.

108. Are you aware of any discussions within the Administration about authorizing warrantless physical searches of individuals' homes or offices within the United States?

Response:

Director Mueller recalls no such discussions.

USA PATRIOT Act

109. In March, Chairman Specter introduced legislation (S. 2369) that contained four additional changes to the Patriot Act, beyond what was in the reauthorization package.

a. In Chairman Specter's bill, the provision relating to Section 215 would require the government to convince a FISA judge: (1) that the business records pertain to a terrorist or spy; (2) that the records pertain to an individual in contact with or known to a suspected terrorist or spy; or (3) that the records are relevant to the activities of a suspected terrorist or spy. Do you agree this standard is adequate to provide agents with the flexibility they need? If not, please provide specific examples demonstrating why not.

Response:

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

b. Another provision would add a four-year sunset to recent changes to the National Security Letter statutes. Given that the sunset would allow existing law to govern any ongoing investigations, do you have any objection to that sunset provision?

Response:

The FBI does not favor a sunset provision, since the revisions of the NSL statutes appear to be reasonable and fair both to the FBI, as the issuer of NSLs, and to NSL recipients. If these provisions prove not to work as intended, they can be revised when that conclusion is reached. Even without a sunset provision, these provisions will no doubt be reevaluated periodically to ensure they are operating as intended, and modifications may be made as needed.

c. Another provision of the bill would make sure that recipients of business records orders under Section 215 of the Patriot Act and recipients of National Security Letters can get meaningful judicial review of the accompanying gag orders. Under the reauthorization package, the recipient would have to prove that any certification by the government that disclosure would harm national security or impair diplomatic relations was made in bad faith. This seems to be a virtually impossible standard to meet. How frequently would you estimate that FBI agents make such certifications in bad faith?

Response:

The bad-faith standard to which this question refers, contained in the USA PATRIOT Improvement and Reauthorization Act of 2005 (hereinafter the "Reauthorization Act"), applies in the very limited context of a petition challenging the nondisclosure provision of a national security letter or a FISA business records order in which there has been a certification by the AG, the DAG, an Assistant AG, or the FBI Director that disclosure of the letter or the business records order may endanger the national security of the United States or interfere with diplomatic relations. We do not expect that any such certifications will be executed in bad faith. We should note, however, that under the statutory scheme contained in the Reauthorization Act, if the government invokes any other reason for nondisclosure (i.e., interference with a criminal, counterterrorism, or counterintelligence investigation or danger to the life or physical safety of any person), even if such a certification is made to that effect by one of the officials enumerated above, or if the certification is made by an official other those enumerated above, then the nondisclosure provision can be set aside if the district court finds there is no reason to believe such damage will occur. Accordingly, the bad-faith standard to which the question refers will be applicable only in a very narrow subset of all cases in which nondisclosure provisions in NSLs or business records orders are challenged. We note that there have only been two such challenges in the history of the NSL statutes (there has been no challenge to a FISA business records order), and none since the USA PATRIOT Act was reauthorized. In one of the two challenges, after the enactment of the Reauthorization Act, the government did not certify that its disclosure would cause harm and the NSL was, in fact, disclosed.

d. Chairman Specter's bill would require that subjects of delayed notice criminal searches be notified of the search within 7 days, unless a judge grants an extension of that time. The bill would leave in place the ability to get unlimited 90-day extensions. Given that the government can obtain unlimited 90-day extensions, why not create a presumption that a citizen should be notified within 7 days if his or her home has been searched by the government?

Response:

Rule 41(f) of the Federal Rules of Criminal Procedure requires the officer who executes a federal search warrant to leave a copy of the search warrant, together with a receipt for all items seized, at the place that was searched. The statute permitting delayed notice, initially enacted as part of the USA PATRIOT Act, is already an exception to the general rule. Delayed notice searches continue to be unusual and are done only when the government can demonstrate good cause for any notification delay We believe the law correctly vests in the issuing judge the authority to determine how long that delay should be.

Terrorist Watch List

110. I understand that the Terrorist Screening Center at the FBI has a redress process but works behind the scenes with other agencies to try to rectify any problems that individuals experience as a result of being mistakenly placed on a terrorist watch list or mistakenly identified as someone on the list. Should people who believe they are adversely affected by the Terrorist Screening Center watch list have the right to appeal an adverse consequence that results from it, and to take their appeal to court? How do we balance the right to appeal with the need for secrecy?

Response:

TSC believes an effective redress process is critical to the public's trust in the United States Government's terrorist screening efforts and the protection of individuals' civil liberties. Therefore, it is essential that those who believe they have been adversely affected by these screening efforts have access to a review process through which errors can be identified and corrected.

When the terrorist screening process adversely affects an individual's important rights, benefits, or privileges, the individual has the right to independent review of the basis for the adverse action. For most such circumstances, a review process is already in place and is tailored to the specific context in which an individual may be affected by terrorist screening. The consolidated watchlist is largely used by agencies that have existing authority to screen individuals and take action on the grounds of terrorist connections or other disqualifying factors. Depending on what action an agency takes as a result of the terrorist screening process, the individual may have a right to a formal agency appeal or to judicial review under the Administrative Procedure Act or other applicable law.

As the question recognizes, the challenge is to balance the need for access to information in the context of an appeal with the need to protect sensitive or classified information that, if released, could undermine the effectiveness of the

consolidated watchlist or the Government's other counterterrorism efforts. In most instances, a watchlist "hit" serves only to alert the screening agency that intelligence information exists suggesting a nexus to terrorism. The screening agency can then obtain and review this intelligence and decide what action is appropriate consistent with its legal authority. When an agency takes adverse action based on the intelligence information, that information and the fact that the consolidated watchlist led the agency to examine that information become part of the agency record supporting the adverse action.

Thus far, the courts have balanced the right to appeal an agency's action with the need for secrecy by conducting *ex parte, in camera* review of any sensitive or classified information that formed the basis for agency action. This process has worked well and should serve as the model for judicial review of adverse actions that flow from the terrorist screening process.

Previous Letters

111. Please respond to a letter I sent you on April 24, 2006, asking for information about FBI policy directives apparently issued in 2003 and 2004 to clarify guidelines regarding investigations that involve public demonstrations or protest activities.

Response:

The FBI's response, dated 5/25/06, is provided as Enclosure B.

112. Please respond to a September 16, 2005, letter that Senator Sununu and I sent to you, asking for follow-up information regarding a GAO report that analyzed the use of data mining technology by the Foreign Terrorist Tracking Task Force.

Response:

The FBI's response, dated 11/25/05, is provided as Enclosure C.

Questions Posed by Senator Schumer

113. The Inspector General reported that the FBI, "as the lead federal agency for preventing and investigating terrorism, has an overarching role in protecting the nation's seaports." (p. 13)

a. Do you agree with that assessment?

Response:

Yes. As the lead federal agency for preventing and investigating terrorism, the FBI has a critical role in protecting the American public and all aspects of our nation's infrastructure. Consistent with HSPD 5 (2/28/03), the FBI exercises lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at United States citizens or institutions abroad, and for related intelligence collection activities within the United States. The FBI is also aware of the responsibilities assigned to the USCG under the Maritime Transportation Security Act of 2002. The FBI is committed to working with our partners in the USCG and other Federal, state, and local agencies to make the United States, our ports, and our inland waters as secure as possible.

b. Nonetheless, the OIG review found serious problems in the allocation of FBI resources and interagency coordination to secure our ports. Do you agree with that OIG assessment?

c. Do you think those deficiencies are acceptable?

Response to subparts b and c:

The FBI engages in the ongoing review of resource allocation and believes its port security resources are properly allocated. The FBI does and will continue to address any identified deficiencies in our operations or our coordination with others. With the benefit of a national MSP management vehicle at FBIHQ and the full-time and collaborative participation in an MSP by the FBI, NCIS, and USCG, the FBI believes interagency coordination is currently effective and continually improving.

d. The OIG made 18 recommendations for improving FBI efforts on port security. Do you intend to follow all of them? If not all, why not?

e. What steps have been taken to follow these recommendations so far?

f. How many remain, wholly or in part, undone?

Response to subparts d-f:

The FBI responded to the OIG report by letter from CTD Assistant Director Willie Hulon to IG Fine dated 3/17/06 (Enclosure A). That letter identifies the steps the FBI has taken and is taking in response to each of the OIG's findings and recommendations. The FBI is preparing a formal reply to the report that

documents these and subsequent steps taken, and this process will be repeated every 90 days until the FBI has completed its response to all report findings and recommendations.

114. While I appreciate all the improvements you are trying to make so that the Sentinel program does not meet the same fate as the Virtual Case File system, I remain concerned about the possibility of a repeat fiasco. I would like to know who is ultimately responsible for this program, success or failure.

a. Specifically, whose job is on the line if this attempt does not work properly?

Response:

The FBI's CIO (Zalmai Azmi) and Program Management Executive (Dean Hall) are responsible for the Sentinel program.

b. The Inspector General has already identified six "continuing concerns" with the Sentinel project. Do you agree with his assessment?

Response:

The DOJ IG outlined seven recommendations in its final pre-acquisition report on Sentinel. The Sentinel PM concurred with those recommendations and had already been taking steps to improve management efforts.

The Sentinel PMO recently received a follow-up "Analysis and Summary of Actions Necessary to Close the Report" from the IG. In that follow-up request, the IG informed the FBI that all seven recommendations are considered "resolved" and will be considered "closed" when specified conditions are met. The Sentinel PMO has submitted a response outlining the actions already taken or, in the case of responsive actions that cannot be completed in the near term, advising what intermediate actions have been taken and when the PMO expects closure.

c. How many of these concerns have been addressed?

Response:

As indicated in response to subpart b, above, the IG has informed the FBI that all seven recommendations are considered "resolved" and will be considered "closed" when specified conditions are met.

d. The IG also points to problems with cost control, though you have apparently developed a tool to track project costs. What exactly is that tool?

Response:

In March 2006, the FBI purchased the wInsight software program. wInsight is an EVM system that will provide early indications of positive or negative variances from planned or scheduled costs. The FBI is also exploring other potential tools to help manage the program. We believe that, while additional tools can help, it is ultimately the responsibility of managers to establish effective policies and procedures and to ensure compliance.

e. Has it been working?

Response:

The wInsight software has been received and data has been loaded, but it is too early to determine the value of the developmental contract. The program will be fully baselined to accommodate EVM and schedule management before development begins.

f. Why has the OIG not been reassured by the existence of this tool?

Response:

We have alerted the OIG that this tool cannot be fully evaluated at this point. We believe that when it can be more fully used, its benefits will be clear to the OIG.

115. An article in *Newsday* pointed out in March that there is another shocking technology gap at the FBI – many agents don't have access to the Internet or Blackberries. The article noted that some FBI agents in New York City did not even have e-mail accounts. The FBI should absolutely have the tools it needs to fight terrorism and crime in the 21st century, most of all in New York City, and one of the most effective means of communications is e-mail and the Internet. FBI agents' not having e-mail or Internet access suggests too much of a pre-9/11 mentality.

a. Do you agree that it is important for FBI agents to be able to communicate with state and local law enforcement through the Internet?

b. Do you agree that the Internet and e-mail are efficient and effective means of enabling this communication?

c. When will FBI agents have access to e-mail and the Internet from their desks?

Response to subparts a-c:

Please see the response to Question 66, above.

116. Among the more disturbing aspects of everything the Inspector General has presented today in his written testimony are his reports of FBI intelligence violations, specifically: FBI agents intercepting communications outside the scope of FISA orders; FBI agents continuing investigative activities after the authority for the investigation expired; and third parties providing information that was not part of a national security letter request. In light of these findings, please explain the following.

a. Were any of these activities that the OIG defines as violations authorized by you, personally, or any deputy of yours?

Response:

No. As indicated in response to Question 60, above, the errors identified by the OIG were either inadvertent or third-party errors. None were the product of directives to exceed FISA or other investigative authority.

b. Were any of these activities authorized by the President?

Response:

No.

c. Does the use of surveillance outside the scope of FISA orders by the FBI have any connection to the NSA domestic surveillance program the President has described? Is it part of a separate program?

Response:

No, in response to each question. As previously stated, the compliance issues noted by the IG were inadvertent, and not wilful, violations.

117. The Inspector General also reports that the OIG found "significant non-compliance" by the FBI with Attorney General guidelines with respect to confidential informants, including "failure to consistently obtain advance approval prior to the initiation of consensual monitoring." This is troubling to me, particularly in connection with the other violations we have discussed and with parts of our intelligence framework that are

apparently out of your control – the NSA program for example. Of course we want strong intelligence, and of course we want you to have the tools you need. However, there is no place for rule-breaking or ducking oversight in our intelligence system.

a. Do you agree?

Response:

The FBI has worked diligently to address this issue and agrees that rule-breaking and ducking oversight have no place in our intelligence system. However, the September 2005 OIG report's findings regarding the FBI's compliance with the AG's investigative guidelines do not include findings regarding the use of confidential human sources or the use of consensual monitoring as investigative techniques.

The OIG report states as follows: "With regard to the Guidelines for conducting nontelephonic consensual monitoring under the AG's Procedures for Lawful, Warrantless Monitoring of Verbal Communications, we found the FBI was largely compliant. However, we found that 10% of the monitoring was recorded prior to obtaining requisite approval." (P. 301.) The OIG made recommendations regarding general consensual monitoring activity for body-wires and nontelephonic transmitters, but these recommendations were not specific to human source operations. The vast majority of these monitoring activities will, by their nature, involve cooperating witnesses who will be expected to testify.

As an investigative technique, consensual monitoring is most often used in criminal investigations. The examples used by the OIG regarding the receipt of approval in advance of consensual monitoring all involved criminal activity rather than intelligence gathering. Pursuant to FBI policy, confidential human sources are not ordinarily used to make consensual recordings or permitted to be present while another individual is conducting consensual recording. In the rare instances when this is desired, it must be approved by a supervisor at the ASAC level or above and the approval must be documented in the confidential human source's file.

This compliance issue is being addressed through the inspection process, training, and the Confidential Human Source Re-engineering Project, which is a collaborative effort between the FBI and DOJ to improve compliance with AG Guidelines and to develop standardized policies and processes for validating and managing confidential human sources. The FBI will use the inspection process to ensure that the required authorizations have been obtained in advance of monitoring and have been appropriately documented. Policy will also provide for the issuance of instructions to the field, including instructions to have

noncompliance addressed in employees' performance appraisals, if appropriate, and to refer egregious noncompliance to OPR.

b. How do you respond to the OIG's findings?

Response:

The FBI welcomes the OIG report and its assessment of our compliance with the four sets of general AG Guidelines that govern our investigative activity. The FBI has made significant progress in designing standardized and automated confidential human source management processes and procedures to be used with respect to all FBI HUMINT. Because we identified many of the OIG's findings in our program self-examination, our re-engineering project has already incorporated most of the OIG's recommendations.

c. What are you doing to stop this pattern?

Response:

The Confidential Human Source Re-engineering Project was initiated to develop standardized policies and processes for managing and validating human sources, thereby improving compliance with AG Guidelines. This re-engineering effort has incorporated most of the OIG's recommendations. The FBI believes these policy changes, along with the IT systems currently under development to automate workflow, will significantly reduce or eliminate noncompliance with AG Guidelines and FBI policies.

The FBI has also begun to implement an improved suite of training in support of human source operations. This effort is being led by the DI, which convened a meeting of FBI training and subject matter experts at a two-week offsite in January 2006 to develop a training plan. Some alterations to New Agent Training have already been implemented. We are also developing an advanced block of human source operations training that we plan to begin implementing by the fall of 2006.

d. What is causing this problem?

Response:

Noncompliance frequently involves exigent circumstances and inadequate understanding of AG Guidelines. Although the vast majority of SAs comply with AG Guidelines, some SAs perceive the policies implemented over the years to be conflicting and to create contradictory or excessively burdensome paperwork

requirements. The development of the FBI's new polices and processes for managing confidential human sources, along with appropriate training regarding these new requirements and clearer consequences for noncompliance, should significantly reduce these incidents.

118. The OIG made 28 recommendations for improving Counterterrorism Task Forces.

a. How many of those do you intend to follow? If not all, why not?

Response:

The FBI intends to follow the 15 of the 28 recommendations that pertain to the FBI. The remaining 13 of the 28 recommendations pertain to agencies other than the FBI. The recommendations that pertain to the FBI are: 2, 5, 6, 7, 8, 16, 17, 18, 19, 20, 21, 22, 23, 24, and 25.

b. What steps have been taken to follow these recommendations so far?

c. How many remain, wholly or in part, undone?

Response to subparts b and c:

The FBI had taken significant steps related to these recommendations even before the IG's report was published. Those steps are articulated in the FBI's response to the report, provided as Appendix XIV to the IG report (Report Number I-2005-007). By letter dated 7/11/06, the FBI provided to the OIG a status report reflecting the actions taken to date with respect to the outstanding recommendations. That report, which is law enforcement sensitive, is provided separately.

Questions Posed by Senator Durbin

FBI Computer Capability
Sentinel Planning

119. As the Sentinel information technology upgrade project commences, what specific management controls have been instituted to prevent a repeat of the problems attendant to the failed "Virtual Case File" deployment? Are there additional safeguards and protocols contemplated? If so, please explain.

Response:

Please see the response to Question 95, above. In addition, please note that, while we do not anticipate that Lockheed Martin will fall short in satisfying its contract obligations, the FBI has established managerial and contractual mechanisms to track contractor performance, including the following.

- A disciplined, stable, and well-conceived program management system that includes strict adherence to the FBI's new IT LCMD and a PMO structure modeled on the program management system successfully used within the Intelligence Community.

- A risk management system under which contract performance risks and the steps being taken to mitigate them are identified on a weekly basis.

- A schedule control and monitoring system pursuant to which variances in the contractor's schedule will be identified every two weeks.

- A requirement that both Lockheed Martin and the Sentinel PMO use a certified EVM system and report on EVM status monthly, identifying baseline variances in cost, schedule, and program performance. Certification of these EVM systems requires IV&V that the system is established and performing in accordance with the national EVM standard.

- A rigorous quality assurance program that includes IV&V of the quality control systems used by both Lockheed Martin and the Sentinel PMO.

- A rigorous configuration and change control system designed to control increases in the scope of technical requirements. Scope changes will not occur unless there is a clear decision by senior executives that the change is necessary and there are adequate time and money in the program schedule and budget to implement the change. The configuration and control system will be focused on preventing unnecessary or inappropriate changes to Sentinel's Statement of Work, the System Requirements Specification, and the Technical Concept of Operations.

- An independent IV&V entity that reports to the FBI's CIO and is responsible for both ensuring that Sentinel's program requirements are valid and verifying that the prime contractor's deliverables meet those requirements.

- An award fee structure that is tied to the performance-based contract performance measurements outlined in the Statement of Work. If contract

performance problems are identified and not rectified, the FBI can reduce the amount of the fee (above contractor cost) awarded Lockheed Martin. In other words, if contract performance is stellar, Lockheed Martin's profit will be greater. If performance is substandard, the profit will be smaller or nonexistent. Also, as indicated above, if the contract performance control mechanisms identify poor contract performance that is not rectified, the Sentinel program is structured so that all or portions of the contract may be terminated.

Sentinel is a "modular build" project, with each of the four phases adding discrete functionality. The initial contract is for Phase 1. The other three phases of Sentinel development, plus O&M support, are not guaranteed work but are, instead, options to be exercised at the discretion of the government based on performance.

120. How are you addressing the various concerns cited by the Justice Department's Inspector General in its March 2006 audit report on pre-acquisition planning pertinent to the Sentinel contract, specifically that:

a. The Sentinel project manager is a CIA employee on loan to the FBI for two years with the possibility of a one-year extension, which could be problematic if he decides to leave before Sentinel is fully installed.

Response:

The Sentinel PM, a CIA employee detailed to the FBI, is committed to serving three years on this program. The FBI is building management depth in the Sentinel program's organization to ensure each part of the PMO includes trained back-up personnel who can ensure the continuity of the program if it should lose an employee, regardless of the employee's position or the reason for loss.

b. The FBI has not yet adequately examined or discussed Sentinel's ability to connect with external systems -- including those in other offices in the Justice Department, the Department of Homeland Security and other intelligence agencies. For instance, the Drug Enforcement Administration, part of the Justice Department, planned to deploy its own new case management system this year and that it is not compatible with Sentinel as currently designed.

Response:

Please see the response to Question 63, above.

c. The FBI planned to finance the computer upgrade by borrowing funds from other FBI programs -- including ones to fight terrorism -- that previously had been appropriated by Congress. The bureau obtained permission to use $97 million from its fiscal 2005 budget for the Sentinel program, including about $29 million from its counter-terrorism division, intelligence-related activities and its cyber division. Diverting substantial funds from such mission-critical areas could begin eroding the FBI's operational effectiveness.

Response:

Please see the response to Question 61, above.

Currently Available Capabilities

121. Your prepared statement describes what tasks an agent at his or [her] computer terminal can perform, but does not explain what they cannot currently accomplish. You testified a few weeks ago before the Senate appropriations subcommittee that in your FY 2007 budget, you are requesting $100 million for Sentinel. You noted that Sentinel will leverage technology to reduce redundancy, eliminate inefficiencies, and maximize the FBI's ability to use the information in its possession. You stressed that the objectives for Sentinel include (1) delivering a set of capabilities that provide a single point of entry for investigative case management and intelligence analysis; (2) implementing a new and improved FBI-wide global index for persons, organizations, places, things, and events; (3) implementing a paperless information management and work-flow capability; and (4) implementing an electronic records management system. Furthermore a story in the May 1, 2006 issue of *The Washington Post* business section mentioned that the Sentinel contract will "link technology systems among the bureau's offices, allowing its agents to search and share information among one another and with other intelligence agencies." I conclude from these statements that agents are still operating in a paper-based case management environment, that search capabilities are not as sophisticated as they could be, and access to information and interchanges are still far short of the potential.

a. Please describe in detail what automated information access capabilities and other functions agents and analysts presently lack on their desktop computers that the Sentinel project is expected to supply? What information remains in paper form and not electronically accessible?

Response:

The automated Sentinel capabilities not presently on an SA's or analyst's desktop include, but are not limited to, electronic workflow management (including electronic document review, approval, and collaboration), enhanced searching of case and intelligence information, information sharing both within the FBI and

with outside entities, and activity reporting. Currently, historical case records, external documents (i.e., court orders), and multimedia formats (i.e., photographs) remain in paper form and, in some cases, are not electronically accessible.

b. What impediments are imposed on agents now that will be alleviated through the Sentinel deployment?

Response:

When Phase 4 is complete, Sentinel will have removed or substantially reduced the following impediments to the FBI's efficiency.

- The cumbersome, inefficient means of accessing case and case-related information, including manual searches of paper case files.
- The need to physically route case and intelligence documents for approval.
- The requirement to manually track, calculate, and report activity metrics.

c. At what points in the deployment of the Sentinel system will various new capabilities be accessible?

Response:

Please see the response to Question 55, above.

OIG Concerns About Information Sharing

122. In March 2006, the Inspector General issued an audit report on "The FBI's Pre-Acquisition Planning For and Controls Over the Sentinel Case Management System." In that report, the Inspector General emphasizes that

> **"the terrorist attacks of September 11, 2001, underscore the need for agencies involved in combating terrorism to be able to communicate with one another effectively. An intelligence agency may have only partial information on a suspected terrorist, but when coupled with information that other agencies possess, a threat may become more clear. "**

Earlier in the report, the OIG noted that the "FBI has expended little effort in assessing information sharing with other federal agencies," that "we have no assurance that the FBI has identified all external systems with which Sentinel must connect" and that "because

these requirements have yet to be established, we anticipate a modification to the contract, [which] represents a potential risk of requirements creep."

a. What is your reaction to these assessments? Are they valid?

Response:

Please see the response to Question 63, above.

b. Wasn't poorly defined and slowly evolving design requirements among the problems contributing to the demise of the Virtual Case File project phase of Trilogy?

Response:

A number of problems contributed to our termination of the VCF project. The FBI has taken care to learn from its mistakes and lay the groundwork for a successful major investment in IT, and the approach to developing Sentinel differs substantially from the VCF approach. For example, Sentinel's requirements and contractual obligations with respect to interfacing with external systems dictate the use of specified standards and best practices. Pursuant to these requirements, when external systems are refreshed, replaced, or enhanced in the ordinary course of their maintenance and upgrading, this will be done using standards compatible with those of Sentinel so that Sentinel systems will be able to communicate with them whether or not their interactions with Sentinel systems were planned initially. This approach and similar approaches to other aspects of the FBI's IT environment will help to minimize "requirement creep."

c. Do you agree that before proceeding too far along on the path of an expensive insular effort, it is essential to account for the necessary sharing relationships both inside and outside the Bureau and the Department, and address critical compatibility issues? How are you addressing this matter?

Response:

We agree that it is important to establish efficient and productive information sharing relationships both inside the FBI and DOJ and with outside entities. For the ways in which Sentinel will optimize these relationships, please see the response to Question 63, above.

d. What components are being incorporated into the Sentinel project to ensure system capacity to afford appropriate access to other agencies within the Intelligence Community?

Response:

Please see the response to Question 63, above.

e. Have there been any changes in the contract to comport with the suggestion of the Inspector General that "the FBI needs to focus more attention on the sharing of information between Sentinel and other agencies' data systems in these early stages of Sentinel's development"?

Response:

Please see the response to Question 63, above.

Sharing & Accessing of Information Beyond the FBI

123. In your prepared statement you acknowledge that in contrast to your optimism about the FBI's ability to successfully function as a leading intelligence agency, others contend that the "FBI is reluctant to share information with its partner agencies."

a. Why do you believe these sentiments abound?

Response:

Although the FBI is now communicating its information sharing policy as clearly, as often, and as broadly as possible, we have not previously focused on the importance of that message. Our policy is to share information with authorized users as a rule and restrict or withhold only by exception. Acting on that policy every day with our many intelligence and law enforcement partners should overcome any remaining perceptions to the contrary.

b. What is your reaction to these criticisms?

Response:

While the FBI is aware of the perception that we may be reluctant to share information with partner agencies, we have also made clear to the Committee that we are pursuing numerous means of improving both the quantity and quality of shared information, doubling the number of IAs and establishing in every field office a FIG in which SAs and analysts work together with one shared mission. In addition, from January 2004 through January 2006 the FBI's IA staffing in the FIGs increased by 61%, helping to fuel our sharing of intelligence products. Since 9/11/01, the FBI has disseminated more than 20,000 intelligence reports, assessments, and bulletins to our partners.

The FBI's commitment to information sharing is also demonstrated in recent organizational changes in the FBI, including the creation of a senior level "Information Sharing Policy Group," chaired by the EAD for the NSB. This Group brings together the FBI entities that generate and disseminate intelligence. Since its establishment in February 2004, this body has provided authoritative FBI policy guidance for internal and external information-sharing initiatives. The FBI shares information and ensures collaboration through our NISS which, along with DOJ's LEISP (of which NISS is a part), aims to ensure that those charged with protecting the public have the information they need to take action. The FBI also participates in the Global Intelligence Working Group and the Global Criminal Intelligence Coordinating Council, which were established in 2004 to set national-level policies to improve the flow of intelligence information among United States law enforcement agencies.

c. How do you propose to change that perspective?

Response:

As the FBI has stated many times, our information-sharing policy is to share with authorized users as a rule and restrict or withhold only by exception. The FBI recognizes that our success in today's threat environment depends on the successes of all of our partners, in both the law enforcement and intelligence communities, and those successes depend on getting the right information into the right hands in a timely manner. For that reason, the FBI will continue to share information as broadly as possible. The FBI has tried to assure our partners of our commitment to broad information sharing, but we understand that actions speak louder than words. Notwithstanding a possible contrary perception, therefore, the FBI will continue to engage in the broadest possible information sharing, because our nation's security depends on it.

FBI/DHS Fingerprint Database Integration

124. What is the current status of the integration effort between the fingerprint databases of the FBI's IAFIS system and Homeland Security's IDENT system?

Response:

With DHS' decision to transition its Automated Biometric Identification System (IDENT) to a 10-print system, the FBI began proactively working with DHS' United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program and other agencies to advance interoperability efforts. In May 2005, principals from DOJ, DHS, and DOS formed an Executive Steering Committee (ESC) to guide the initiative to make IDENT and the FBI's Integrated Automated

Fingerprint Identification System (IAFIS) interoperable, creating an Integrated Project Team (IPT) structure to carry out the design, development, and implementation of an integrated information sharing solution. Under the direction of the ESC, the IPT has made progress toward achieving an interoperability solution that fully addresses interagency requirements. The IPT has completed a Concept of Operations and continues to design options for an interoperable biometric system as a foundation for information sharing based on positive identification. In addition, the IPT has identified high-level interoperability business requirements based upon the needs of IDENT and IAFIS users. These requirements are being analyzed and refined to draft functional and technical requirements needed for design development. The IPT has also identified key policy issues regarding the biometric-based sharing of criminal history and immigration history information related to agency-specific business processes and mission operations, as well as legislative mandates. The mitigation strategies necessary to resolve these issues are being discussed by IPT representatives, as well as subject matter experts within the Departments.

IDENT/IAFIS interoperability is being planned in phases: 1) Interim Solution, 2) Initial Operating Capability (IOC), and 3) Full Operating Capability (FOC). Initially, the FBI and US-VISIT will focus on developing a prototype capable of sharing, in near real time, biometric data on FBI wants and warrants, DOS Category One Visa Refusals, and DHS expedited removals. Full interoperability, which will be achieved through implementation of the IOC and FOC phases, includes sharing all biometric data and would allow agencies to access associated biographic information as allowed by law and policy.

The first step in implementing the interim solution is complete. On November 30, 2005, the FBI began the transfer of all new or updated IAFIS want or warrant records associated with FBI numbers to DHS/US VISIT, on a day-forward basis, to strengthen the screening processes at DOS consulates and DHS ports-of-entry. Before this change, the FBI transferred IAFIS records on wanted persons with a foreign or unknown place of birth, foreign or unknown citizenship, or previous immigration charge. The second step toward implementation of the interim solution is the interagency joint development of an interim Data Sharing Model (iDSM) that will allow a reciprocal sharing of biometric data subsets between IDENT and IAFIS in "near real time" beginning in September 2006.

125. What is the prognosis and timetable for achieving fuller integration and cross-matching capabilities between IDENT and IAFIS?

Response:

As indicated above, the iDSM deployment is scheduled for September 2006. A phased development plan for interoperability between IDENT and IAFIS has been adopted by the IPT to assure that the interoperability implementation schedule maintains technical alignment with the rollouts of the FBI's Next Generation IAFIS initiative, the DHS' IDENT Modernization effort, as well as the DHS transition to 10-print initiative over the next four years.

126. What impediments hinder the IDENT/IAFIS integration effort and how do you suggest that they be overcome?

Response:

The best method for sharing data between IDENT and IAFIS is still to be determined by the Interoperability IPT. A joint cost benefit analysis is currently being conducted by US-VISIT and the FBI's CJIS Division in an effort to identify the best means of exchanging data between the two systems.

127. What catalysts would resolve the delays and accelerate progress of the IDENT/IAFIS integration?

Response:

The President's FY 2007 budget supports the progress of the IDENT/IAFIS integration effort and Congressional support of the President's request would help both agencies make progress on this project.

128. Are reported concerns (*Government Computer News*, 8/29/05) that (1) "despite continued references in official documents to the integration of the two systems, they can never be fully merged" and that (2) "parts of IAFIS contain information classified at a higher level than IDENT users are allowed to access" valid ones? How do you recommend that these issues be resolved?

Response:

The IPT is considering multiple models to identify the best method for exchanging information. The IPT is also analyzing special handling requirements for protected individuals within each model.

129. Now that a key policy discrepancy has been alleviated with the 10-print decision announced in July 2005 by Department of Homeland Security Secretary Michael Chertoff, have you or your designees discussed the operational issues directly with Secretary

Chertoff or any of his designees? If so, with what outcome? If not, do you anticipate discussions in the near term?

Response:

Executive Management from the FBI's CJIS Division has established a strong working relationship with the Executive Management from the DHS/US-VISIT Program and DOS. As mentioned previously, representatives from these agencies lead the Interoperability ESC and have formed an IPT. ESC Meetings are conducted regularly to discuss the interoperability effort, as well as the transition to 10-print collection.

130. What further role can the FBI play to facilitate the integration process?

Response:

In order to facilitate the integration process, the FBI must maintain its current level of commitment to the interoperability effort. In addition to extensive agency participation within the interoperability IPT, collaborative efforts to obtain the support of advisory stakeholders have been a top priority of US-VISIT and the FBI's CJIS Division. For instance, representatives of the IPT attend regular working group and subcommittee meetings of the CJIS Advisory Policy Board (APB) to update interoperability progress and to obtain approval of planned efforts. The IPT has received positive stakeholder support from the APB on its interoperability efforts, as evidenced by the appointment of a DHS representative to the APB. In December 2005, the APB endorsed the current interoperability efforts.

USA PATRIOT Act

131. Section 5 of the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (Public Law 109-178), "Privacy Protections for Library Patrons," is intended to clarify that the FBI may not issue National Security Letters to libraries that are functioning in their traditional role, including but not limited to, lending books, providing access to books or periodicals in digital form, and providing basic access to the Internet. During the debate on the USA PATRIOT Act Additional Reauthorizing Amendments Act, Senator Sununu, the legislation's author and lead sponsor, and I engaged in a colloquy on the floor of the Senate to make clear congressional intent in this respect. During the hearing, my staff provided a copy of this colloquy to your staff. I have also attached a copy of the colloquy to these questions. During the hearing, I asked you if you agreed that Section 5 clarifies that a library functioning in its traditional role is not subject to a National Security Letter. You promised to respond in writing to this question. Please do so.

Response:

Pursuant to 18 U.S.C. § 2709, the FBI has always been limited in the entities on which it can serve NSLs. In the context of this particular question regarding libraries, an NSL can only be served on an entity that is an electronic communication service provider. The FBI has always understood an electronic communication service provider to be an entity that provides electronic communication services as defined by 18 U.S.C. § 2510(15). Thus, a library is only subject to an NSL if it provides electronic communication services.

Section 5 of the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (Public Law 109-178), "Privacy Protections for Library Patrons," states that a library functioning in its traditional role, statutorily defined as including the provision of access to the Internet, is not subject to an NSL unless the service it provides meets the definition of an electronic communication service, as defined in 18 U.S.C. § 2510(15). As the above makes clear, the FBI believes Section 5 did not actually change the law.

Immigration Background and Name Checks

132. The processing of many applications for immigration benefits involves a background check by the FBI, including a criminal history check based on the applicant's name ("name check"). Please describe the background check and name check process.

Response:

Several million name check requests are received by the FBI each year, and we continue to work to complete our review of a batch of 2.7 million requests submitted by USCIS in December 2002. The FBI's NNCP receives most USCIS name check requests by way of a magnetic data tape that can hold up to 10,000 names. When a data tape is received, the names on the tape are electronically checked against the FBI's UNI. These searches seek all instances in which the individual's name appears in both "main" files and "reference" files. If the individual's name appears in a "main" file, the individual is, himself, the subject of an FBI investigation, whereas the individual's inclusion in a "reference" file indicates only that the person's name appears in an FBI investigation. "References" may be associates, conspirators, or witnesses.

The majority of the names submitted on a data tape are electronically checked and returned to USCIS as having "no record" within 48 to 72 hours. A "no record" result indicates that the FBI's UNI database contains no identifiable information regarding the individual. Duplicate submissions (i.e., identically spelled names

with identical dates of birth submitted within the last 120 days) are not checked, and the duplicate findings are returned immediately to USCIS.

If the database does contain identifiable information regarding the individual, a secondary manual name search is conducted. These manual searches typically result in " no record" results within 30 to 60 days, and the USCIS is so advised. The remaining name checks (usually about 10% of those originally submitted) are identified as possibly being the subject of an FBI record. At this point, the FBI record must be retrieved and reviewed. If the record is available in the FBI's electronic record keeping system, it can be reviewed quickly. If not, the relevant information must be retrieved from an existing paper record. Review of this information is necessary to determine whether the information is positively identified with the name check requested. If the information is not identified with the request, the request is closed as a "no record," and the requesting agency is so notified.

The average time required to retrieve and review an FBI record for possible information related to a name check request depends on the number of files an analyst must obtain (which is dictated by the number of "hits" on a name), the location and availability of those files, and the amount of information contained in each file. If a file is available electronically or stored locally, the analyst will be able to obtain the file within a matter of days. If, instead, the file is located in one of over 265 different FBI locations that can house information pertinent to a name check, the file must be requested, and this process may take considerably longer.

Ultimately, less than 1% of the requests are identified with files containing possible derogatory information. If such information is located, the FBI forwards a summary to the USCIS, which adjudicates the matter (the FBI does not adjudicate applications for immigration benefits).

133. During the hearing, I asked you about delays in FBI background checks and name checks for applicants for immigration benefits. You said that you would provide statistics on these delays. Please provide the following:

a. A statistical breakdown by time periods of delay.

Response:

The current pending name checks submitted by USCIS are broken down as follows:

	0-30 Days	31-60 Days	61-90 Days	91-120 Days	Over 120 Days	Over 1 Year
Total USCIS Name Checks	36888	45026	31746	13934	68411	106011

b. A statistical breakdown of the delays for different types of immigration applications.

Response:

	0-30 Days	31-60 Days	61-90 Days	91-120 Days	Over 120 Days	Over 1 Year
Asylum Program	2485	3144	2349	512	3229	2977
Waivers and Misc.	1201	1604	1256	345	6556	5634
Exec Office of Immigr. Review	1096	1265	1783	752	1465	20
Naturalization	15431	21582	11941	6857	25975	44843
Personnel Security	10	4	4	1	123	464
Adjustment of Status	16665	17427	14413	5467	31063	52073
TOTALS	36888	45026	31746	13934	68411	106011

c. A statistical breakdown of the delays by the applicants' country of origin.

Response:

The NNCP does not track incoming USCIS name checks by country of origin, but it does attempt to process USCIS name checks on a first-in, first-out basis, unless USCIS requests that a given request be expedited.

134. a. How does the FBI relay information regarding a completed background check to U.S. Citizenship and Immigration Services?

Response:

The FBI relays information regarding a completed background check to USCIS in a couple of ways. Batch USCIS name check requests that are submitted on a magnetic data tape that result in a "no record", which means that the FBI's

Universal Index database contains no identifiable information regarding a particular individual, are returned on a magnetic data tape. If an expedited name check request results in a "no record", the result is faxed to USCIS. The results of a name check other than "no record" are provided to USCIS in a writing (paper based) and sent to USCIS Headquarters via FedEx.

b. Have there been any cases in which the FBI has completed a background check but, due to miscommunication, CIS mistakenly believes that the check has not been completed? If yes, what has been the cause for the miscommunication and what can be done to ensure such miscommunications do not take place in the future?

Response:

The FBI's NNCP personnel do not recall an instance where the results of a name check were transmitted to USCIS Headquarters, and through a miscommunication, USCIS Headquarters continued to believe the name check was still pending. The FBI is not familiar with how name check results are provided to USCIS field offices once the information is provided to USCIS Headquarters. The FBI Name Check staff and the USCIS Headquarters staff communicate on a daily basis regarding the status of name checks. Additionally, USCIS Headquarters staff receive a summary of all quarterly responses to insure accuracy regarding the status of a completed name check.

135. Does the FBI have a process for expediting background checks for applications that have been pending for a long period of time? If not, should there be such a process?

Response:

The policy of the FBI's NNCP is to process the oldest name checks first. Customer agencies, such as USCIS, may request expedited handling of specific name checks. The criteria used to determine which name checks will receive expedited handling are established by the submitting agency, including USCIS, and are not developed or evaluated by the FBI. The FBI does request that the number of expedited cases be kept to a minimum in fairness to those awaiting the results of other pending name check requests. The FBI's policy is to be responsive to our customers' needs within the limits of our resources.

ENCLOSURE A

QUESTIONS 68 AND 113

3/17/06 LETTER FROM CTD AD WILLIE HULON TO DOJ IG GLENN FINE

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

March 17, 2006

The Honorable Glenn A. Fine
Inspector General
Office of the Inspector General
United States Department of Justice
Room 4322
950 Pennsylvania Avenue, Northwest
Washington, D.C. 20530

Dear Mr. Fine:

I would like to thank you for providing the Federal Bureau of Investigation (FBI) the opportunity to respond to your report entitled, "The FBI's Efforts to Prevent and Respond to Maritime Terrorism."

I recognize the substantial challenge the Office of the Inspector General (OIG) has in producing timely reports on complex issues such as this. This challenge is even more difficult when assessing FBI operations because of the rapid changes it continues to undergo to optimally position itself to address the evolving threats to our Nation.

In large part, the FBI agrees with the findings and recommendations of this report. Accordingly, Executive Management from the Counterterrorism Division (CTD) of the FBI and personnel from the appropriate programs within the FBI have reviewed OIG's draft report concerning the FBI's efforts to prevent and respond to maritime terrorism. Ideally, we would like for the report to be updated to provide a current status of maritime security efforts in the FBI, and to that end have set forth several points of information for you to consider.

- The FBI initiated the Maritime Security Program (MSP) in July 2005. This proactive measure was taken by CTD Executive Management in recognition of the potential threat of maritime terrorism. It is worth noting that this program was established without additional funding by reallocating resources within CTD.

- Availability of resources has also influenced the FBI's participation in various exercises. Although the FBI would like to participate in additional exercises, the FBI is currently able to support the joint exercises that are coordinated through the National Exercise Program.

- The FBI is actively working with the United States Coast Guard (USCG) and other agencies to resolve potential coordination issues in advance of actual threats and incidents in the maritime domain.

Mr. Glenn A. Fine

Additionally, the following comments are to correct or clarify statements made in the text of the audit report:

4. Page "v", first paragraph and page 25, first paragraph: The MSP prepared an Electronic Communication (EC) to the field to request that an FBI Special Agent (SA), as opposed to a Task Force Officer (TFO) be designated as the primary Maritime Liaison Agent (MLA). Although this EC was drafted, it was not approved by CTD management. As a result, in many Field Offices a TFO serves as the primary or only MLA.

5. Page "vi", first bullet: This point may need to be modified to include the capabilities of the Laboratory Division's Hazardous Materials Response Unit (HMRU) in dealing with a weapon of mass destruction (WMD) incident. HMRU provides technical and scientific operational response to WMD incidents, including, but not limited to, crime scene management, evidence recovery, emergency decontamination and scientific assessments. The responsibilities of the Hazardous Devices Response Unit (HDRU) includes the response to threats and actual devices before they are detonated or used in an "attack." HDRU does not respond to post-detonation attacks; that is the responsibility of HMRU and/or the Laboratory Division's Explosive Unit.

6. Page "viii", last paragraph: The statement, "The FBI has not collected complete data on the number of suspicious activities or terrorist threats involving seaports," is correct. However, the MSP has begun to collect this information from all available sources. The MSP has created a data base to capture this information which will be used to identify and track possible trends in suspicious activity at ports and port facilities. The MSP is also in the process of creating a standardized reporting mechanism for use by the MLAs when responding to incidents. These reports will be maintained in the MSP case file and the information will also be entered into the data base. Finally, the MSP maintains liaison with other agencies and the private sector, such as the USCG, Office of Naval Intelligence (ONI) and the International Council of Cruise Lines (ICCL), for the sharing of pertinent threat information.

7. Page 20, bottom of the page: It should be noted that the MSP will present the 2006 Maritime Liaison Agent Training Conference in Long Beach, California from 04/03-07/2006. The Port of Long Beach is one of the busiest ports in the United States with a variety of inter-modal transportation systems. This site was specifically chosen because it offers hands on/familiarization training using various port facilities and vessels. The curriculum for this conference is expected to include presentations on the impact of maritime directives under the National Strategy for Maritime Security (NSMS); informant and liaison development; legal issues; enhancing maritime domain awareness; the FBI's capabilities and resources to respond to a maritime incident; and guidance to the field on best practices.

8. Page 24, first full paragraph: The report indicates that as a result of placing responsibility for managing the MLA Program under the MSP, all of the FBI's transportation related counterterrorism programs are located within the same

organizational unit. This is not the case as the National Joint Terrorism Task Force (NJTTF) initiated the Rail Liaison Agent (RLA) Program via EC dated 10/24/2005. The NJTTF requested each Field Office to designate an FBI SA or TFO as a primary and secondary RLA. A separate initiative is currently underway to evaluate the feasibility of creating a program or unit focused on all aspects of the transportation sector. It is important to note this initiative is unfunded and would be created by reallocating existing resources.

9. Page 24, last paragraph: The report mentions that one of the objectives of the MSP was to create a website on the FBI's Intranet to facilitate the dissemination of information pertaining to directives, training, intelligence and other matters. This objective has been accomplished. The MSP website address is http://ctd.fbinet.fbi/semu/maritime/. This website contains information on maritime directives including National Security Presidential Directive (NSPD)-41/Homeland Security Presidential Directive (HSPD)-13, the NSMS and key supporting plans; maritime related statutes; intelligence reports; points of contact; and links to related programs including the Directorate of Intelligence (DI), and the Office of the General Counsel (OGC). Information is continually updated or added to the website. The MLAs are notified of information posted to the website via e-mail. The website has generated positive feedback from the MLAs and is a readily available source of standardized information for the field.

10. Page 24, last paragraph: The report also mentions that another objective of the MSP was to review maritime related suspicious activity reports to identify any trends that may be indicative of pre-operational planning. As noted above, the MSP has already started this process, which is ongoing. This effort is complicated by the lack of standardized reporting and difficulty in retrieving this information, as stated elsewhere in the findings.

11. Page 25, middle of the page: The report states that the MSP has not reviewed the eight supporting plans under the NSMS to identify the FBI's responsibilities nor identified all of the FBI's representatives assigned to the corresponding working groups. That information was supplied to OIG at the inception of the MSP. Since then, the MSP has thoroughly reviewed NSPD-41/HSPD-13, the NSMS and all eight of the supporting plans. The FBI's responsibilities under these directives have been identified and are being addressed. NSPD-41/HSPD-13, the NSMS and key supporting plans are posted to the MSP website. Due to limited resources, the MSP must prioritize which of the working groups to attend in support of these efforts. In that regard, representatives from the MSP have regularly attended and participated in the Maritime Security Policy Coordinating Committee (in support of Executive Management); the Maritime Security Working Group; the Maritime Operational Threat Response (MOTR) Implementation Team; and the Maritime Domain Awareness Implementation Team. In addition, an interagency MOTR Joint Working Group (JWG) has recently been established to address the planning, standardization and exercise requirements that will be deleted from the final version of the MOTR Plan as the Homeland Security Council has indicated. The MSP participates in this JWG as well as the Border and Transportation Security Policy Coordinating Committee.

Mr. Glenn A. Fine

12. Page 25, fourth paragraph: The report states neither the MSP's FY 2006 goals and objectives nor the critical duties of an MLA include the need for the FBI to develop relationships with people who can inform the FBI about maritime operations. It should be noted that at the time the MSP's goals and objectives were established (via EC dated 08/19/2005), the MSP did not have responsibility for managing the MLA Program. In fact, the first objective identified in that EC was to coordinate with the NJTTF to assume responsibility for the MLA Program. That objective was accomplished on 10/04/2005, when the MSP assumed responsibility for managing the MLA Program.

Furthermore, within the goals and objectives (via EC dated 08/19/2005), the MSP established various objectives for the field. One of these objectives was to "ensure effective liaison between the MLA and various law enforcement agencies, port and shipping officials in respect to counterterrorism preparedness." In the goals and objectives EC, the MSP identified five core competencies which included the establishment of a human intelligence base.

Finally, in an EC to all Field Offices dated 07/12/2004, the NJTTF stated, "The goal of the MLA Program is to enhance the maritime environment through increased interaction between MLA members, private industry, state and local port authorities, to include law enforcement and other federal agencies with maritime responsibilities. These enhancements will result from the establishment of close working relationships between the MLAs and concerned entities within the maritime field…" The EC goes on to provide additional guidance and an extensive list of recommended liaison contacts, including participation in the local Area Maritime Security Committee (AMSC). In addition to these specific recommendations, every FBI SA, including those designated as MLAs, are evaluated on specific critical elements. One of the core critical elements for all FBI SAs is the development of an intelligence base, which includes source development. This process encompasses identifying, initiating and developing relationships with individuals or organizations that may provide information or assistance in investigations and assignments. Therefore, CTD believes the need for the FBI to develop relationships with people who can inform the FBI about maritime operations has been thoroughly addressed.

As you requested, the MSP has provided responses to pertinent recommendations. Additionally, recommendations not under MSP's purview were provided to the appropriate offices, (i.e., the DI, the Critical Incident Response Group (CIRG), and CTD's Counterterrorism Analysis Section.) Responses to the recommendations are set forth below.

Recommendation #1

OIG Recommendation: Ensure that MLA guidance is consistent with the actual role of MLAs.

FBI Response: FBI agrees with this recommendation. The MSP has already made significant progress in this regard.

Through the creation of the MSP website, which contains information on maritime directives, including NSPD-41/HSPD-13, the NSMS and key supporting plans; maritime related statutes; intelligence reports; points of contact; and links to related programs including the DI and the

OGC. Information is continually updated or added to the website. The MLAs are notified of information posted to the website via e-mail. The website has generated positive feedback from the MLAs and is a readily available source of standardized information for the field.

The MSP is in the process of planning the 2006 Maritime Liaison Agent Training Conference in Long Beach, California from 04/03-07/2006. This site was specifically chosen because the Port of Long Beach is one of the busiest ports in the United States with a variety of inter-modal transportation systems. The conference will include hands on/familiarization training using various port facilities and vessels. The curriculum for this conference is expected to include presentations on the impact of maritime directives under the NSMS; informant and liaison development; legal issues; enhancing maritime domain awareness; the FBI's capabilities and resources to respond to a maritime incident; and guidance to the field on best practices.

Finally, now that the MSP has responsibility for management of the MLA Program, the MSP will establish specific, quantifiably measurable and attainable goals and objectives that are consistent with the responsibilities assigned to the MLAs, to include recommendations for participation in various local working groups and liaison contacts.

Recommendation #2

OIG Recommendation: Assign MLAs based on an assessment of the threat and risk of a terrorist attack to critical seaports.

FBI Response: FBI agrees with this recommendation. FBI will ensure that resources are assigned or available necessary to address the risk or threat based on the assessment.

Recommendation #3

OIG Recommendation: Measure the amount of resources devoted to maritime efforts by establishing a maritime case classification under the general Counterterrorism Preparedness classification.

FBI Response: FBI agrees with this recommendation. The MSP has already taken certain steps which would enhance the FBI's ability to measure the amount of resources devoted to maritime efforts.

FBI is in the process of establishing a classification for maritime matters.

In August 2005, the MSP provided recommendations to the Counterintelligence Division for changes to the Investigative Accomplishment Report (FD-542) to capture activity conducted in support of the MLA Program. Finalization of the modifications to this report are pending.

Recommendation #4

OIG Recommendation: Require field offices to name at least one MLA to each AMSC.

FBI Response: FBI agrees with this recommendation. FBI will ensure that adequate resources are dedicated to each Area Maritime Security Committee to address priority matters.

Mr. Glenn A. Fine

Recommendation #5

OIG Recommendation: Require field offices to immediately notify the Maritime Security Program of any MLA appointments or reassignments.

FBI Response: FBI agrees with this recommendation. The MSP updates the MLA list on a regular basis. The MLA list is maintained by the MSP and is available on the MSP web site. The list identifies, by Field Office, all of the MLAs as well as the JTTF Supervisors who have oversight of the MLA Program. The list provides contact information, identifies if the MLAs are assigned to a Resident Agency (RA) and which ports they cover. The MSP has advised field offices to immediately notify the MSP of any personnel changes affecting the MSP, and this guidance will be reiterated through training such as the 2006 Maritime Liaison Agent Training Conference.

Recommendation #6

OIG Recommendation: Ensure that the Maritime Security Program has measurable objectives.

FBI Response: FBI agrees with this recommendation and recognizes that significant changes and progress in the MSP require the establishment of more specific, quantifiably measurable and attainable goals and objectives.

While FBI recognizes that the goals and objectives established for the MSP (via EC dated 08/19/2005) did not include quantifiable measures, it should be noted that the MSP was a new program and no previous goals and objectives had been established. Furthermore, the MSP did not have responsibility for managing the MLA Program at the time the initial objectives were established. The first objective of the MSP was to coordinate with the NJTTF to assume responsibility for the MLA Program.

It is also worth noting that the NSMS and all of the supporting plans were released in the final quarter of 2005, after the date on which these objectives were established. Final directives under the NSMS have not been established, even as of the date of this response. Under these circumstances, it is difficult to quantify the amount of training and/or reference materials required to train MLAs in the field.

Despite the lack of specific, quantifiably measurable objectives at the inception of the program, the MSP accomplished several of the stated objectives, including the following:

- The MSP assumed responsibility for managing the MLA Program on 10/04/2005;
- Training and reference materials to assist the MLAs have been distributed via e-mail, posted to the FBI's Intranet, and will be presented at the 2006 Maritime Liaison Agent Training Conference scheduled to take place 04/03-07/2006;
- The MSP established a web site on the FBI's Intranet where current information including, but not limited to, maritime directives, statutes and intelligence is maintained;
- The MSP continually identifies, analyzes and disseminates information pertaining to maritime threats, vulnerabilities and safety/security issues;

- The MSP continually coordinates with other programs within the FBI to enhance situational awareness for the MSP, other programs, FBIHQ and the field;
- The MSP has already begun to review and track suspicious activity reports to determine if there are any trends which could indicate terrorist activity and has disseminated information to the field in this regard; and
- The MSP is actively engaged in liaison with other government agencies as well as the private sector. This effort and the fact that the MSP serves as a primary point of contact and a coordination center within the FBI for maritime issues has enhanced the FBI's liaison with these groups.

Recommendation #7

OIG Recommendation: Ensure that the Maritime Security Program's objectives include developing human intelligence.

FBI Response: FBI agrees with this recommendation and asserts that the MSP and the NJTTF have already provided such guidance to the MLAs.

As stated above, at the time the MSP's goals and objectives were established, the MSP did not have responsibility for managing the MLA Program. Even so, the MSP established various objectives for the field. One of these objectives was to "ensure effective liaison between the MLA and various law enforcement agencies, port and shipping officials in respect to counterterrorism preparedness." In the goals and objectives EC, the MSP identified five core competencies which included the establishment of a human intelligence base.

Prior to the existence of the MSP, in an EC to all Field Offices dated 07/12/2004, the NJTTF stated, "The goal of the MLA Program is to enhance the maritime environment through increased interaction between MLA members, private industry, state and local port authorities, to include law enforcement and other federal agencies with maritime responsibilities. These enhancements will result from the establishment of close working relationships between the MLAs and concerned entities within the maritime field…" The EC goes on to provide additional guidance and an extensive list of recommended liaison contacts, including participation in the local AMSC.

In addition to these specific recommendations, every FBI SA, including those designated as MLAs, are evaluated on specific critical elements. One of the core critical elements for all FBI SAs is the development of an intelligence base, which includes source development. This process encompasses identifying, initiating and developing relationships with individuals or organizations that may provide information or assistance in investigations and assignments. Therefore, FBI believes the need for the FBI to develop relationships with people who can inform the FBI about maritime operations has been thoroughly addressed.

The MSP also plans to address liaison and the development of a human intelligence base during the 2006 Maritime Liaison Agent Training Conference which is scheduled for 04/03-07/2006. In addition, the MSP will include specific recommendations to the MLAs in the objectives which will be established for FY 2007.

Mr. Glenn A. Fine

Recommendation #8

OIG Recommendation: Ensure that the FBI's MOTR operations plan examines high risk scenarios, determines the required response time, and evaluates how FBI resources would address the scenarios.

FBI Response: The FBI's maritime operational response plan takes into account various high-risk scenarios to include the criminal/terrorist use of biological, chemical or radiological WMD, as well as Improvised Explosive Devices (IEDs)and Improvised Nuclear Devices (INDs). Other high-risk scenarios include a large number of hostages on a maritime platform and/or the involvement of sophisticated criminal/terrorist adversaries. The TSB's tactical response to maritime threats mirrors the response to any other tactical response. That is, the FBI tactical response is a tiered approach which recognizes that local field offices will respond as necessary (Tier 1), with regional response (Tier 2) added as the evaluation of the situation may dictate. National response, as required (Tier 3), will involve the deployment of the Hostage Rescue Team (HRT), as well as other FBI SWAT teams and possibly the HDRU and the Laboratory's HMRU, as the scenarios would necessitate. Response times vary as a consequence of venue. HRT, HDRU and HMRU response times are typically notification plus four hours for deployment in addition to any travel time involved to the specific venue.

Recommendation #9

OIG Recommendation: Establish a requirement for joint FBI/Coast Guard exercises in field offices assessed as having high-risk seaports.

FBI Response: CIRG will require the fourteen (14) field offices that have been given enhanced tactical maritime training to make overtures to the USCG to conduct joint exercises on an annual basis. It should be noted that the FBI is not in a position to require USCG participation, however, the FBI will extend the invitation to the USCG as well as to other appropriate entities.

Recommendation #10

OIG Recommendation: Resolve potential role and incident command conflicts in the event of a maritime terrorist incident through joint exercises and, if necessary, a revised and broadened MOU with the Coast Guard.

FBI Response: FBI concurs in stating that this is currently being addressed through the revision of the final interagency MOTR Plan. It may be premature to determine if a revised memorandum of understanding (MOU) with the USCG will be necessary until the final MOTR Plan has been approved and vetted through exercises and/or operations. Again, the FBI is not in a position to require the USCG to enter into a renewed MOU.

Recommendation #11

OIG Recommendation: Prepare after-action reports after all maritime-related exercises and use the reports to identify and disseminate lessons learned and best practices.

FBI Response: This is being addressed in a separate joint initiative within the FBI. It is anticipated an After Action Report (AAR) template will be developed that applies to all critical incidents, special events and exercises. CIRG's Crisis Management Unit (CMU) is responsible

Mr. Glenn A. Fine

for program oversight for the production of AARs per the Manual of Investigative and Operational Guidelines (MIOG), Part 2, section 30-1.8 (1) (a), (b) and (c) which specifically sets out the requirements for AARs.

Recommendation #12

OIG Recommendation: Ensure that all field offices submit critical incident reports to the CIRG by January 15 each year; require the FBI's Maritime Security Program, in consultation with the CIRG, to use the reports to conduct maritime-specific reviews of the FBI's crisis management policies and practices — including any requirements for field office crisis management plans — and to disseminate maritime-related lessons learned and best practices.

FBI Response: CIRG's CMU ensures adherence to the MIOG's Part 2, section 30-1.8 which requires that field offices submit critical incident reports to CIRG by January 15th of each year. CTD's MSP will provide information concerning maritime related lessons learned and best practices.

Recommendation #13

OIG Recommendation: Assess the threat and risk of maritime terrorism compared to other terrorist threats and ensure the National Threat Assessment ranks the various modes of attack and targets.

FBI Response: FBI will ensure that intelligence gaps are identified and action is initiated to resolve any deficiencies.

Recommendation #14

OIG Recommendation: Ensure the amount of FBI resources dedicated to maritime terrorism is based on the extent of the maritime threat in relation to other threats.

FBI Response: FBI agrees with this recommendation. FBI will ensure that adequate resources are allocated to address priority threats.

Recommendation #15

OIG Recommendation: Monitor the progress of operating divisions and field offices in answering intelligence collection requirements pertaining to seaports and maritime terrorism.

FBI Response: The Directorate of Intelligence will provide a response to this recommendation.

Recommendation #16

OIG Recommendation: Focus intelligence reporting to more comprehensively address potential maritime-related terrorist targets and methods.

FBI Response: The Directorate of Intelligence will provide a response to this recommendation.

Recommendation #17

Mr. Glenn A. Fine

OIG Recommendation: Name a unit within the Counterterrorism Division to monitor the volume and substance of all FBI maritime-related intelligence.

FBI Response: FBI Counterterrorism Division will ensure that Maritime related intelligence as well as investigations are monitored and properly managed.

Recommendation #18

OIG Recommendation: Consider establishing a requirement for regular field office intelligence bulletins to summarize the field office's suspicious incident reporting and, if such a requirement is adopted, establish standardized frequency, content, and distribution requirements.

FBI Response: The Directorate of Intelligence will provide a response to this recommendation.

The FBI has prepared the appropriate responses to the recommendations found in your report. The responses have undergone a classification review (Enclosure 1) and Sensitivity Review (Enclosure 2).

The responses were coordinated through the FBI's Inspection Division. Please contact Shirlene Savoy of the Inspection Division should you have any questions. Ms. Savoy can be reached at (202) 324-1833.

I want to thank you again for your efforts in producing this report, and I welcome the opportunity to discuss in detail the progress the FBI continues to make in this area.

Please contact me should you have any questions regarding this matter.

Sincerely yours,

Willie T. Hulon
Assistant Director
Counterterrorism Division

ENCLOSURE B

QUESTION 111

5/25/06 LETTER
FROM FBI OFFICE OF CONGRESSIONAL AFFAIRS
TO SENATOR FEINGOLD

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

May 25, 2006

The Honorable Russell D. Feingold
United States Senate
Washington, DC

Dear Senator Feingold:

I am writing in response to your April 24, 2006 letter to Director Robert S. Mueller, requesting copies of policy directives mentioned in a March 14, 2006 FBI press release. By letter dated March 31, 2006, Chairman Pat Roberts requested copies of the same documents on behalf of the Senate Select Committee on Intelligence (the "SSCI"). By cover dated April 28, 2006, the FBI furnished the SSCI with copies of the referenced directives, as well as two additional directives that provide further context for the responsive materials. It is our understanding that these documents are now available for review by Senators and staff with appropriate clearances. We hope you and your staff will find these materials helpful.

In your letter, you also inquired whether the directives cited in the March 14, 2006 FBI press release are the same as those documents cited on pages 196-197 of the September 2005 Office of Inspector General ("OIG") report entitled, "The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines." In sum, there is substantial overlap between the documents referenced in the March 2006 press release and those cited in the OIG's September 2005 report. All but one document cited by the OIG (namely, the April 2004 communication concerning "Special Events") are among the materials referenced in the FBI press release and subsequently provided to the SSCI. The documents furnished to the SSCI, however, also include two directives not cited by the OIG (one is classified; the other post-dates the documents cited by the OIG).

Finally, your letter asks for an explanation of the process that led the FBI to issue these directives and the details of any incidents that may have prompted these clarifications. The directives in question consist of six separate documents. Two of the directives were issued to provide initial guidance on new or revised Attorney General guidelines. The remaining four documents were issued to emphasize and clarify existing policies. None of the directives references specific incidents or operations. Rather, the documents reflect an ongoing dialogue between FBI Headquarters and FBI field offices, designed to underscore and complement the regular guidance provided to employees by the field-based legal advisors, known as Chief Division Counsels.

The Honorable Russell D. Feingold

We appreciate this opportunity to respond to your inquiry. Again, we hope you and your staff will find the materials furnished to the SSCI helpful and informative.

Sincerely,

Eleni P. Kalisch

Eleni P. Kalisch
Assistant Director
Office of Congressional Affairs

ENCLOSURE C

QUESTION 112

11/25/05 LETTER
FROM FBI OFFICE OF CONGRESSIONAL AFFAIRS
TO SENATE COMMITTEE ON THE JUDICIARY

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

November 25, 2005

Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

I am writing in response to a letter dated September 16, 2005 from Senator Feingold on behalf of the Subcommittee on the Constitution, Civil Rights and Property Rights seeking information in support of the Subcommittee's oversight activity relating to recent reviews by the Government Accountability Office (GAO) of government-wide data mining projects. Senator Sununu joined in Senator Feingold's letter.

Enclosed is relevant information concerning the FBI data mining efforts referenced in the GAO reports. If the Committee has additional questions that are not addressed in the enclosed materials, we will work with your staff to schedule a briefing by appropriate FBI officials.

Please do not hesitate to contact this office if we can be of assistance regarding this or any other matter.

Sincerely yours,

Eleni P. Kalisch

Eleni P. Kalisch
Assistant Director
Office of Congressional Affairs

Enclosure

Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Honorable Arlen Specter

Honorable Sam Brownback
Chairman
Subcommittee on the Constitution, Civil
Rights and Property Rights
Committee on the Judiciary
United States Senate
Washington, DC 20510

Honorable Russell D. Feingold
Ranking Member
Subcommittee on the Constitution, Civil
Rights and Property Rights
Committee on the Judiciary
United States Senate
Washington, DC 20510

Honorable John E. Sununu
United States Senate
Washington, DC 20510

The Federal Bureau of Investigation's Foreign Terrorist Tracking Task Force, Investigative Data Warehouse, and Intelligence Community Data Marts

The Government Accountability Office's (GAO) May 2004 report addresses three FBI programs: the Foreign Terrorist Tracking Task Force (FTTTF), Investigative Data Warehouse (IDW) (which is the successor to the Secure Collaborative Operational Prototype Environment (SCOPE)), and Intelligence Community Data Marts (ICDM). The August 2005 GAO report further focused on the efforts of the FTTTF to locate foreign terrorists and their supporters in the United States. While the term "data mining" has been defined in various ways, the FBI typically uses this term to mean "advanced analysis" or the ability to work with large amounts of data quickly and in ways that were previously not possible computationally due to size or speed limitations. The FBI uses the FTTTF, IDW, and ICDM to search multiple sources for information in support of the FBI's mission of analyzing intelligence in order to detect terrorist activity. All three programs can be used to conduct "criterion" searches, in which they search for all entries that meet multiple criteria (including such criteria as names and other personal identifiers).

FTTTF

The mission of the FTTTF is to provide to law enforcement and intelligence community agencies information that helps keep foreign terrorists and their supporters out of the United States or that leads to their location, surveillance, detention, prosecution, or removal. The FTTTF uses data mining tools to search large amounts of data, including open-source data, to provide law enforcement and intelligence partners with actionable intelligence. FTTTF analysts and others in the FBI access commercial databases only in accordance with applicable Attorney General Guidelines to search for information about individuals and groups in whom the FBI has a valid investigative interest. Information developed by the FTTTF is forwarded through the National Joint Terrorism Task Force to the Joint Terrorism Task Forces (JTTFs) for follow-up.

While the FTTTF searches data maintained by both government and commercial sources under appropriate circumstances, with only one exception it uploads into FBI systems (or "ingests") only government data sets. Some of these government data sets are acquired on a one-time basis and others are acquired periodically as they are updated by the originator. In all cases, the acquisition of a government data set is based on specific operational needs. Although the FTTTF does not ingest entire commercial data sets (with one exception, as noted below), it does have access to information held and maintained by commercial data providers pursuant to agreements with these providers. The FTTTF accesses this commercially available data remotely through specific queries, ingesting only the results of the query for purposes of analysis. The one commercial data set ingested by the FTTTF, which was added to the FTTTF due to the technical

limitations of the provider's system, consists of name, telephone number, and address information (i.e., an electronic telephone book).

The nature of a database query will depend on the information available at the time of the query. For example, if the FTTTF were to receive an appropriate request from a law enforcement or intelligence agency for information about one or more named individuals suspected of being foreign terrorists traveling within the United States, those names would be run through the FTTTF system and appropriate commercial data sources to obtain information on the individuals. If, instead, the FTTTF were to receive a proper request to search only information as to age, gender, country of birth, citizenship, and a specific travel pattern during a given time frame, a query would be conducted against only government databases to narrow the inquiry to specific names or personal identifiers. The search results from these government databases (a list of names or personal identifiers) could then form the basis for a query against appropriate commercial sources.

FBI investigators do not base actions or investigative conclusions on a sole fact obtained from a database. Instead, they use information obtained from both internal and external data sources as pieces of information, or "building blocks," that assist them in developing a complete investigative picture. For example, if an investigator needs information in the possession of a certain John Brown, a database may be used to locate Mr. Brown, to distinguish this John Brown from others with the same name, or even to develop questions to be used in interviewing Mr. Brown, but the database information alone would not provide a basis for arrest or similar actions. The FTTTF reduces false positive identifications through a thorough vetting protocol that is external to the FTTTF data system, pursuant to which all query results are reviewed and analyzed by highly skilled analysts. The resulting analyses are provided to operational law enforcement and national security investigators as "leads"; that is, as information those investigators can use to develop additional, actionable information. For this reason, while it is important that the FBI have access to accurate information in order to develop effective investigative strategies, investigative conclusions are not based solely on database search results.

The use of FBI data mining systems must comport with applicable Attorney General Guidelines for criminal and intelligence investigations, which permit searches for information about individuals and groups in whom the FBI has a valid investigative interest. FTTTF systems have been certified and accredited in accordance with FBI policy, and training ensures users are familiar with the appropriate usage of these systems. The FTTTF's combined access to Department of Homeland Security border information, information provided by other government agencies, FBI investigative data, and commercially available information (such as public-source data) has enabled it to evaluate more than 60,000 individuals for associations with terrorism since January 2005, resulting in the provision of more than 100 leads to JTTFs.

Section 208 of the E-Government Act of 2002, Public Law 107-347, requires that agencies conduct Privacy Impact Assessments (PIAs) for information technology systems that collect, maintain, or disseminate identifiable information regarding individuals, but exempts

national security systems from the PIA requirement. While the FTTTF system is a national security system, and is therefore exempt from the section 208 PIA requirement, FBI PIA guidelines require that a PIA be completed for any new system that collects, maintains, or disseminates information about individuals, and do not exempt national security systems. A PIA has, consequently, been conducted for the FTTTF system pursuant to these FBI PIA guidelines. The PIA incorporates the requirements of both section 208 and the implementing Office of Management and Budget (OMB) guidelines. Just as section 208 does not require that PIAs be conducted for national security systems, its requirement for publication of the PIA is also inapplicable to national security systems.

The FBI has made substantial progress implementing GAO's August 2005 recommendations. The FTTTF has applied information security measures, obtaining the Security Division's "authorization to operate," and is developing and testing a contingency plan in preparation for certification and accreditation in accordance with national security standards. In addition, as noted above, the FBI has conducted a PIA, as required by FBI PIA guidelines, incorporating the requirements of Section 208 of the E-Government Act of 2002 and OMB's implementing guidelines. Pursuant to FBI PIA guidelines, the FTTTF system has been reviewed and approved by the FBI's Senior Privacy Official acting in conjunction with the FBI's Privacy Council. While the FTTTF system is a national security system and is, therefore, exempt from the publication requirements of the E-Government Act, the FBI is reviewing the circumstances under which it might make this information available to the public while protecting classified and other law enforcement sensitive information.

IDW

As a consequence of the terrorist attacks of September 2001, the FBI identified the need to develop tools that could serve broader FBI investigative needs by accessing myriad data sources previously not readily available using conventional software tools. SCOPE was the initial prototype effort designed to support counterterrorism initiatives. The SCOPE prototype succeeded in enhancing FBI investigative and analytical capabilities, and it soon became a key asset for nearly 500 FBI operational users. Subsequently, the IDW project was initiated, building upon the successes of the SCOPE prototype and extending its operational capabilities to a larger number of users.

The IDW program's mission is to provide a one-stop shop through which agents and analysts can develop investigative leads from a variety of data sources related to counterterrorism, counterintelligence, cyber, and criminal investigations. This information includes numerical data, text, graphics, illustrations, imagery, photos, audio, and video that can be accessed in near real time using a single web-based interface that operates independent of the location of the user and the data source. Before the development of IDW, the same information was accessible, but it had to be acquired through stand-alone, individual sources and manually aggregated. The IDW includes security features that facilitate the sharing of data among

authorized users (while preventing unauthorized access) and the auditing of users' activities to detect rogue users.

IDW is used to search only data sets that have been ingested into IDW. These data sources include primarily FBI and other government information, such as information provided by the Departments of Justice, Homeland Security, State, and Treasury, but they also include some open-source newspaper articles related to counterterrorism. IDW is not used to search outside data, including outside public-source information maintained in commercial data bases. IDW is designed to consolidate the information obtained through these searches into reports that can be disseminated for operational use both within the FBI and to appropriate outside federal, state, and local agencies.

As indicated with respect to the FTTTF, FBI PIA guidelines require that a PIA be completed for any new system that collects, maintains, or disseminates information about individuals, and a PIA has been conducted for IDW. The use of FBI data mining systems must also comport with applicable Attorney General Guidelines for criminal and intelligence investigations, which permit searches for information about individuals and groups in whom the FBI has a valid investigative interest, and IDW has been certified and accredited in accordance with FBI policy.

ICDM

While the ICDM was only in the planning stages when the May 2004 GAO report was drafted, elements of this initiative have since been deployed. The ICDM builds on the tools in IDW and uses IDW as a data source, searching a subset of IDW information. As is true with respect to IDW, ICDM does not query commercial databases. ICDM will operate both internally (working with real-time intelligence feeds in support of FBI analysts) and externally (sharing FBI intelligence products with appropriate agencies), providing for the near real-time provision of relevant data to analysts based on areas of interest and alerting recipients to high-priority incoming information. ICDM will link directly to IDW and provide a common web-based portal work environment, supporting queries to other databases as one means of reducing the problems inherent in stovepipe systems. Currently, ICDM is being used internally by select FBI analysts as part of the FBI Automated Messaging System. Externally, ICDM currently supports direct web-based access to other agencies' classified systems, including the Secret Internet Protocol Router Network and the secret-level INTELINK system, from any FBINET workstation. Both the internal and external ICDM systems are undergoing Operational Readiness Review and are expected to transition to full operations near the end of 2005.

As with both the FTTTF and the IDW, a PIA has been conducted for the ICDM and the ICDM has been certified and accredited in accordance with FBI policy.

SUBMISSIONS FOR THE RECORD

United States Government Accountability Office

GAO

Testimony

Before the Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m. EDT
Tuesday, May 2, 2006

FEDERAL BUREAU OF INVESTIGATION

Weak Controls over Trilogy Project Led to Payment of Questionable Contractor Costs and Missing Assets

Statement of Linda M. Calbom, Director
Financial Management and Assurance

GAO
Accountability * Integrity * Reliability

GAO-06-698T

May 2, 2006

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-698T, a testimony before the Committee on the Judiciary, U.S. Senate

FEDERAL BUREAU OF INVESTIGATION

Weak Controls over Trilogy Project Led to Payment of Questionable Contractor Costs and Missing Assets

Why GAO Did This Study

The Trilogy project—initiated in 2001—is the Federal Bureau of Investigation's (FBI) largest information technology (IT) upgrade to date. While ultimately successful in providing updated IT infrastructure and systems, Trilogy was not a success with regard to upgrading FBI's investigative applications. Further, the project was plagued with missed milestones and escalating costs, which eventually totaled nearly $537 million. This testimony focuses on (1) the internal controls over payments to contractors, (2) payments of questionable contractor costs, and (3) FBI's accountability for assets purchased with Trilogy project funds.

What GAO Recommends

GAO's related report (GAO-06-306) makes 27 recommendations to help improve (1) FBI's and the General Services Administration's (GSA) controls over their invoice review and approval processes and to address questionable billing issues and (2) FBI's accountability for assets. FBI concurred with GAO's recommendations. GSA accepted the recommendations but expressed concern with some of the findings and one recommendation. GAO reaffirms its position on all of its findings and recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-698T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda M. Calbom at (202) 512-9508 or calboml@gao.gov.

What GAO Found

FBI's review and approval process for Trilogy contractor invoices, which included a review role for GSA as contracting agency, did not provide an adequate basis for verifying that goods and services billed were actually received and that the amounts billed were appropriate, leaving FBI highly vulnerable to payments of unallowable costs. This vulnerability is demonstrated by FBI's payment of about $10.1 million in questionable contractor costs we identified using data mining, document analysis, and other forensic auditing techniques. These costs included first-class travel and other excessive airfare costs, incorrect charges for overtime hours, potentially overcharged labor rates, and charges for which the contractors could not provide adequate supporting documentation to substantiate the costs purportedly incurred.

FBI also failed to establish controls to maintain accountability over equipment purchased for the Trilogy project. These control lapses resulted in more than 1,200 missing pieces of equipment valued at approximately $7.6 million that GAO identified as part of its review. The table below summarizes questionable contractor costs and missing assets that GAO identified.

Questionable Costs and Missing Assets

Dollars in thousands

Issues identified	Amount
First-class travel	$20.0
Excessive air travel costs	49.8
Excess overtime charges	400.0
Potential overcharging of labor rates	2,100.0
Inadequately supported subcontractor labor costs	1,957.9
Inadequately supported other direct costs	5,508.3
Duplicate payment of subcontractor labor invoice	26.3
Total questionable costs	**$10,062.3**
1,205 pieces of missing equipment	$7,607.1

Source: GAO.

Given the poor control environment and the fact that GAO reviewed only selected FBI payments to Trilogy contractors, other questionable contractor costs may have been paid that have not been identified. If these control weaknesses go uncorrected, future contracts, including those related to Sentinel—FBI's new electronic information management system initiative—will be greatly exposed to improper payments. In addition, the lack of accountability for Trilogy equipment calls into question FBI's ability to adequately safeguard its existing assets as well as those it may acquire in the future.

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to discuss the results of our audit of the Federal Bureau of Investigation's (FBI) internal controls over contract payments related to the Trilogy project and safeguarding assets purchased with Trilogy funds. Our recently issued report,[1] developed at the request of this committee, identifies weaknesses in FBI's ability to establish and implement controls that reasonably ensure, among other things, that goods and services billed were actually received and that the amounts billed were appropriate. Further, our report also discusses how FBI failed to establish controls to maintain accountability over equipment purchased for the Trilogy project. These weaknesses resulted in payment of millions of dollars in questionable contractor costs and missing assets. It is imperative that FBI correct these weaknesses in order to avoid similar outcomes for its Sentinel and other information technology (IT) projects.

Before I get into our audit findings, let me first provide some brief background on the Trilogy project. For several years, FBI's IT systems were considered archaic and inadequate for efficiently and effectively investigating criminal and other cases. Initiated in mid-2001, Trilogy—FBI's largest IT upgrade to date—was intended to modernize FBI's IT infrastructure and systems and provide needed applications to help FBI agents, analysts, and others do their jobs. The Trilogy project consisted of two primary efforts—upgrades to FBI's IT infrastructure[2] and development of an investigative application system to more efficiently access case files, which became known as the Virtual Case File (VCF) system. FBI entered into an interagency agreement with the General Services Administration (GSA), which served as the contracting agency to acquire the services of two primary contractors to carry out the Trilogy project. DynCorp—now Computer Services Corporation (CSC)—was responsible for the IT infrastructure upgrade, while Science Applications International Corporation (SAIC) was responsible for development of the VCF system. In addition, FBI contracted with Mitretek to assist in the administration and oversight of the project.

[1] GAO, *Federal Bureau of Investigation: Weak Controls over Trilogy Project Led to Payment of Questionable Contractor Costs and Missing Assets*, GAO-06-306 (Washington, D.C.: Feb. 28, 2006).

[2] The IT infrastructure portion of Trilogy consisted of two parts: (1) upgrades to FBI's computer hardware and software and (2) upgrades to FBI's communication network.

Although the original scheduled completion date for the overall Trilogy project was June 2004, after September 11, 2001, FBI instituted an accelerated deployment plan. The targeted completion date for the portion of Trilogy related to FBI's IT infrastructure was accelerated from May 2004 to July 2002. However, after several delays the upgrade was completed in April 2004, only a month before the "pre-accelerated" due date.

While the scheduled completion date for the VCF system was originally June 2004, the due date for the first VCF deliverable was accelerated to December 2003. However, in July 2004, the VCF portion of the Trilogy project was scaled back after the completion of the first phase of the project was determined to be infeasible and cost prohibitive as originally envisioned. The scaled back VCF effort was recast as a pilot that ended in March 2005, and was to be used by FBI to help develop requirements for a successor information management system initiative, referred to as Sentinel. The overall cost of the Trilogy project, originally estimated at approximately $380 million, ultimately escalated to approximately $537 million.

The Department of Justice Office of Inspector General has reported on numerous issues that contributed to the cost increases and delays, including poorly defined and slowly evolving design requirements, contracting weaknesses, unrealistic task scheduling, and lack of management continuity and oversight for tracking and overseeing costs effectively.[3] We also earlier reported on weaknesses in FBI's IT systems development and management capabilities, including contractor oversight.[4] Because of these issues, you asked us to audit the costs of the Trilogy project, the majority of which represented the purchase of goods and services from contractors. Our objectives were to determine whether (1) FBI's internal controls provided reasonable assurance that payment of unallowable contractor costs would not be made or would be detected in the normal course of business,[5] (2) FBI's payments to contractors were

[3] Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*, Report No. 05-07 (Washington, D.C.: February 2005).

[4] See for example, GAO, *Information Technology: FBI Is Building Management Capabilities Essential to Successful Systems Deployments, but Challenges Remain*, GAO-05-1014T (Washington, D.C.: Sept. 14, 2005).

[5] Unallowable costs are contractor costs that are not allowed under a term or condition of the contract or pursuant to applicable regulations.

properly supported as a valid use of government funds, and (3) FBI maintained proper accountability for assets purchased with Trilogy project funds.

We performed our work in accordance with generally accepted government auditing standards in Washington, D.C., and at two FBI field sites and various other GSA and contractor locations in Virginia. The complete scope and methodology of our review is discussed in appendix II of our report.[6]

Today, I will summarize the results of our work with respect to (1) weaknesses in FBI's internal controls that made it highly vulnerable to payment of unallowable or questionable contractor costs with Trilogy funds, (2) certain payments for questionable contractor costs that we identified, and (3) FBI's inadequate accountability for assets purchased with Trilogy project funds.

Insufficient Invoice Review and Approval Process Increased FBI's Vulnerability to Payment of Unallowable Contractor Costs

FBI's review and approval process for Trilogy contractor invoices, which was carried out by a review team consisting of officials from FBI, GSA, and Mitretek, did not provide an adequate basis for verifying that goods and services billed were actually received by FBI or that payments were for allowable costs. This occurred in part because responsibility for the review and approval of invoices was not clearly defined or documented. In addition, contractor invoices frequently lacked detailed information required by the contracts and other additional information that would be needed to facilitate an adequate review process. Despite this, invoices were paid without requesting additional supporting documentation necessary to determine the validity of the charges. These weaknesses in the review and approval process made FBI highly vulnerable to payment of unallowable or questionable contractor costs.

While the invoice review and approval process differed for each contractor and type of invoice charge, in general the process carried out by the review team lacked key procedures to reasonably ensure that goods and services billed were actually received by FBI or that the amounts billed and paid were for allowable costs. For example, the review team did not have a systematic process for verifying that the individuals listed on labor invoices actually worked the number of hours billed or that the job

[6] GAO-06-306.

classification and related billing rates were appropriate. Further, there was no documented assessment of whether overall hours billed for a particular activity were in line with expectations. In addition, the review team paid contractor invoices for subcontractor labor charges without any attempt to assess the validity of the charges. The GSA official responsible for paying the invoices stated that the review team relied on the contractors to properly bill for costs related to subcontractors and to validate the subcontractor invoices. However, the review team had no process in place to assess whether the contractors were properly validating their subcontractor labor charges or to assess the allowability of those charges.

The insufficient invoice review and approval process was at least in part the result of a lack of clarity in the interagency agreement between FBI and GSA as well as in FBI's oversight contract with Mitretek. We have identified the management of interagency contracting as a high-risk area, in part because it is not always clear with whom the responsibility lies for critical management functions in the interagency contracting process, including contract oversight.[7] For example, the terms and conditions of the interagency agreement with GSA only vaguely described GSA's role in contract administration. In particular, the agreement did not specify the invoice review and approval steps to be performed or who would perform them. Likewise, the Mitretek contract provided a general description of Mitretek's oversight duties, but did not specifically mention its responsibilities related to the invoice review and approval process. Additionally, the lack of clarity in roles and responsibilities was evident in our interviews with the review team, where each party indicated that another party was responsible for a more detailed review.

The failure to establish an effective review process was compounded by the fact that not all invoices provided the type of detailed information required by the contracts and other information that would be needed to validate the invoice charges. For example:

- CSC labor invoices did not include information related to individual labor rates or indicate which overhead rates were applicable to each employee—information needed to verify mathematical accuracy and to determine that the components of the labor charges were valid.
- CSC invoices provided a summary of travel charges by category (e.g., airfare and lodging), but did not provide required information related to an

[7] GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

individual traveler's trip costs. The travel invoices also did not provide cost detail by travel authorization number. Therefore, there was no way to determine that the trips billed were approved in advance or that costs incurred were proper and reasonable based on the location and length of travel.

- CSC and SAIC invoices for the other direct costs (ODC) provided a summary of charges by category (e.g., shipping and office supplies); however, CSC did not provide required cost detail by transaction. In some cases, the category of charges was not even identified. For example, as shown in figure 1, on the ODC invoice, a category entitled "Other Direct Costs" made up $1.907 million of the $1.951 million invoice current billing total. No additional information was provided on the invoice to explain what made up these costs.

Figure 1: Example of CSC ODC Invoice

No explanation provided for these costs that made up almost 98% of the invoice charges

DynCorp I&ET, Inc

[redacted]

Contract: GS00T99ALD20204 **Task:** T0001AJM026

CLIN 0003A OTHER DIRECT COSTS
Period of Performance: March 26, 2002 - April 25, 2002

Category	Current Billing	Cumulative Billing
Local Travel - Mileage	$145.05	$5,691.10
Local Travel - Parking	$66.00	$1,922.23
Freight/Shipping	$4,595.27	$31,581.92
Direct Materials		$1,370.72
FacCharges/Telephones		$212.04
Interco -Costs	$24,999.98	$104,166.67
Office Supplies		$6,436.44
Other Direct Costs	$1,907,077.75	$1,985,916.75
Other Reproduction, Printing	$1,563.54	$3,187.71
Software		$709.85
Travel-Other		$718.34
Materials & Supplies	$12,973.78	$14,721.25
Postage		$12.45
Outside Services/Other		$0.00
Rentals - Equipment		$285.03
Training - Materials		$657.14
Total ODCs	**$1,951,421.37**	**$2,157,589.64**
[redacted]	[redacted]	[redacted]
TOTAL	[redacted]	[redacted]

Source: CSC (previously DynCorp).

Even though contractor invoices, particularly those from CSC, frequently lacked key information needed for reviewing charges, we found through inquiries with the review team and the contractors that invoices were generally paid without requesting additional supporting documentation.

We further found that invoices for equipment did not individually identify each asset being billed by bar code, serial number, or some other identifier that would allow verification of assets billed to assets received. This severely impeded FBI's ability to determine whether it had actually received the assets included on invoices and to subsequently track individual accountable assets on an item-by-item basis.

Some Payments Made to Contractors Were for Questionable Costs

Because of the lack of fundamental internal controls over the process used to pay Trilogy invoices, FBI was highly vulnerable to payment of unallowable contractor charges. In order to assess the effect of these vulnerabilities, we used forensic auditing techniques to select certain contractor costs for review. We identified about $10.1 million in questionable contractor costs paid by FBI. These costs included payments for first-class travel and other excessive airfare costs, incorrect billings for overtime hours worked, potentially overcharged labor rates, and other questionable costs. Given FBI's poor control environment over invoice payments and the fact that we reviewed only selected FBI payments to Trilogy contractors, other questionable costs may have been paid that have not been identified.

First-class Travel and Other Excessive Airfare Costs

During our review of CSC's supporting documentation for selected travel charges, we found 19 first-class airline tickets costing a total of $20,025. The CSC contract called for travel to be reimbursed to the extent allowable under the Joint Travel Regulations, which state that travelers must use basic economy or coach class unless the use of first-class travel is properly authorized and justified. Because the documentation provided by CSC for these first-class tickets we identified did not contain the required authorizations or justifications, we consider the cost of this travel in excess of coach-class fares as potentially unallowable.[8]

[8] The determination of unallowable costs is made by the contracting agency. Therefore, until such determination is made, we have categorized these costs as potentially unallowable.

Also during our review of travel charges, we noted several instances of unusually expensive coach-class tickets, which we also considered to be questionable. Upon further inquiry with several airlines, we determined that most of these were for "full fare" coach-class tickets. We noted that the airlines used most often by the contractors indicated that it is possible to obtain a free upgrade to first class with the purchase of the more expensive full-fare coach ticket. In fact, we found that in some instances, the current price of a full-fare coach ticket was higher than the current price of a first-class ticket. We noted 62 full-fare coach tickets billed by CSC for $85,336. In contrast, we estimated that basic coach-class fares would have cost $41,978. SAIC and Mitretek also billed FBI for excessive airfare costs, but to a lesser degree. In total, we identified 75 unusually expensive tickets costing $100,847, which exceeded our estimate of basic coach-class fares by approximately $49,848. Table 1 provides examples of the first-class and excessive airfare travel costs we identified.

Table 1: Examples of First-class and Excessive Airfare Travel Costs

Contractor	Itinerary	Ticket class	Actual cost of ticket	Estimated cost of basic coach-class ticket[a]	Percentage that full-fare coach exceeded basic coach cost
CSC	Chicago, IL to Pittsburgh, PA and back	First-class	$926	$197	370
Mitretek	Washington, DC to Phoenix, AZ and back	First-class upgrade[b]	2,051	480	327
CSC	One-way from Los Angeles, CA to Philadelphia, PA	Full fare	1,253	307	308
CSC	One-way from Las Vegas, NV to Washington, DC	Full fare	1,171	304	285
CSC	One-way from San Francisco, CA to Cleveland, OH	Full fare	1,049	290	262
Mitretek	Washington, DC to Portland, OR and back	First-class upgrade[b]	1,850	643	188
CSC	One-way from San Diego, CA to Baltimore, MD	Full fare	1,128	413	173
CSC	Wichita, KS to Washington, DC and back	First-class	1,984	732	171
CSC	Atlanta, GA to Los Angeles, CA and back	Full fare	2,121	851	149
SAIC	Denver, CO to Washington, DC and back	Not determinable[c]	1,570	1,037	51

Source: GAO analysis of supporting documentation provided by contractors.

[a]Because historical costs for coach-class tickets were not available, we estimated the costs of coach-class tickets based on an average of current prices for a similar itinerary purchased 3 days in advance (which was the average based on the trips we reviewed) and adjusted for inflation applicable to airfare.

[b]The fare basis code for this ticket indicated that a first-class upgrade was obtained. We could not verify whether this ticket was purchased as a full-fare coach or some other class of travel that exceeded the basic coach-class fares.

[c]We could not determine the airfare class of the ticket purchased because the supporting documentation provided did not include the fare basis code.

Excess Overtime Charges

Our review also showed that FBI may have paid SAIC for incorrectly billed overtime charges. The task order for SAIC work stated that the government would not object to SAIC employees working hours in excess of 40 per week if necessary. In March 2003, SAIC implemented a policy that FBI agreed to, which decreased the amount of hours that would be billed to FBI. This policy stated that contractor staff would be compensated for hours worked that exceeded 90 hours in a 2-week pay period, and established a ceiling of 120 hours per pay period. We found,

however, that SAIC employees frequently charged for all hours worked beyond 80 in a pay period and noted some instances where employees charged hours beyond the 120-hour ceiling. The costs of these hours were billed to and paid by FBI. SAIC management acknowledged that billings were not consistent with the March 2003 policy and indicated that it would research the issue further to determine whether corrections are necessary.[9] Based on our review of the labor charges, FBI may have overpaid for more than 4,000 hours. Using average, fully burdened labor rates for employees who billed incorrectly, we estimated that FBI may have overpaid these overtime costs by as much as $400,000.

Questionable Labor Rates

We also found that CSC/DynCorp may have charged labor rates that exceeded ceiling rates that GSA asserts were established pursuant to a DynCorp task order. In short, GSA and CSC disagree on whether ceiling rates for a CSC/DynCorp subcontractor, DynCorp Information Systems (DynIS), were ever established. When DynCorp entered into the contractual agreement with GSA, it agreed to ceiling rates for various labor categories and agreed to negotiate subcontractor ceiling rates separately for each task order. The May 2001 DynCorp task order award document stated that ceilings were in place on all DynIS labor category and indirect rates, subject to negotiation pending the results of a Defense Contract Audit Agency[10] audit. GSA officials told us they believed that DynIS labor category rates in DynCorp's Trilogy proposal represented established ceilings, and that they negotiated DynIS labor category ceiling rates with DynCorp. However, CSC stated that it never negotiated labor category ceiling rates with GSA.

Based on our review of DynCorp's labor invoices, we noted that several of DynIS's rates charged exceeded the labor rates that GSA contended were ceiling rates. For example, CSC/DynCorp billed over 14,000 hours for work performed by senior IT analysts during 2001 on the Trilogy project based on an average hourly rate of $106.14. However, if ceiling rates were

[9] SAIC officials indicated that in June 2003 a waiver of the 10 hours of uncompensated time associated with the overtime policy was implemented for select teams. However, SAIC could not provide us information on which teams, tasks, or employees the waiver applied to or the length of time the waiver covered. Therefore, we were not able to consider this waiver in our analysis.

[10] DCAA is responsible for performing all contract audits for the Department of Defense. They also provide contract audit services to other government agencies when hired to do so.

established, the DynCorp proposal indicated that the Trilogy project would be charged a maximum of $68.73 per hour for a senior IT analyst working in the field or $96.24 per hour for a senior IT analyst working at headquarters during 2001. If ceiling rates were established, we estimated that FBI overpaid CSC/DynCorp by approximately $2.1 million for DynIS labor costs.

Other Questionable Costs

We also identified about $7.5 million in other payments to contractors that were for questionable costs. In most cases, these costs were not supported by sufficient documentation to enable an objective third party to determine if each payment was a valid use of government funds. For example, CSC did not provide us adequate supporting documentation for almost $2 million of subcontractor labor charges and about $5.5 million of ODC charges we selected to review.

Because $4.7 million of these inadequately supported ODC costs were for training charges from one subcontractor, CACI Inc. – Federal (CACI), we subsequently requested supporting documentation from the subcontractor for selected charges for training costs totaling about $3.5 million. We found that CACI could not adequately support charges to FBI totaling almost $3 million that CACI paid to one event planning company (another subcontractor). CACI stated that supporting documentation was not applicable because its agreement with the event planner was "fixed priced." However, CACI's assertion was not supported by the terms of the purchase order and related statement of work that specifically required documentation to support costs claimed by the event planner and to charge only for services rendered.

CSC was also unable to provide us adequate supporting documentation for $762,262 in equipment disposal costs billed by two subcontractors. The documentation provided consisted of a spreadsheet that summarized costs of the subcontractors, but did not include receipts or other support to prove that these costs were actually incurred.

Our review of SAIC's subcontractor labor charges found that FBI was billed twice for the same subcontractor invoice totaling $26,335. SAIC officials agreed that they double billed and stated that they would make a correction.

Major Lapses in Accountability Resulted in Millions of Dollars of Missing Trilogy Equipment

Our audit also disclosed that FBI did not adequately maintain accountability for equipment purchased for the Trilogy project. FBI relied extensively on contractors to account for Trilogy assets while they were being purchased, warehoused, and installed. However, FBI did not establish controls to verify the accuracy and completeness of contractor records it was relying on. Moreover, once FBI took possession of the Trilogy equipment, it did not establish adequate physical control over the assets. Consequently, we found that FBI could not locate over 1,200 assets purchased with Trilogy funds, which we valued at approximately $7.6 million. Because of the significant weaknesses we identified in FBI's property controls, the actual amount of missing equipment could be even higher.

FBI relied on contractors to maintain records related to the purchasing, warehousing, and installation of about 62 percent of the equipment purchased for the Trilogy project.[11] FBI's primary contractor responsible for delivering computer equipment to FBI sites was CSC. FBI officials told us they met regularly with CSC and its subcontractors to discuss FBI's equipment needs and a deployment strategy for the delivery of equipment. Based on these meetings, CSC instructed its subcontractors to purchase equipment, which was subsequently shipped to and put under the control of those same subcontractors. Once equipment arrived at the subcontractors' warehouses, the subcontractors were responsible for affixing bar codes on accountable items—all items valued above $1,000 and certain others considered sensitive that are required by FBI policy to be tracked individually. In addition, FBI directly purchased about $19.1 million of equipment for the Trilogy project that was shipped directly to either CSC or CSC subcontractors.

When equipment was shipped from a subcontractor warehouse to an FBI site, the subcontractor prepared a bill of lading that listed all items shipped. However, there was no requirement for FBI officials to verify that the items were actually received. The subcontractors also prepared a "Site Acceptance Listing" of equipment that had been installed at each FBI site. While an FBI official signed this listing, based on our inquiries at two field offices, we found the officials may not have always verified the accuracy and completeness of these lists. FBI did not prepare its own independent lists of ordered, purchased, or paid-for assets and did not perform an

[11] This includes Trilogy equipment purchased by CSC and SAIC and equipment purchased directly by FBI that was delivered to CSC for the IT infrastructure portion of the project.

overall reconciliation of total assets ordered and paid for to those received. Such a reconciliation would have been made difficult by the fact that invoices FBI received from CSC did not include item-specific information—such as bar codes, serial numbers, or shipping location. However, failure to perform such a reconciliation left FBI with no assurance that it had received all of the assets it paid for.

In addition, equipment that was delivered to FBI sites was not entered into FBI's Property Management Application (PMA) in a timely manner, increasing the risk that assets could be lost or stolen without detection. We found that 71.6 percent of the CSC-purchased equipment that was recorded in PMA, representing 84 percent of the total dollar value, was entered more than 30 days after receipt, and nearly 17 percent of the equipment, representing 37 percent of the dollar value, was entered more than a year after receipt. When assets are not timely recorded in the property system, there is no systematic means of identifying where they are located or when they are removed, transferred, or disposed of and no record of their existence when physical inventories are performed. This severely limits the effectiveness of the physical inventory in detecting missing assets and in triggering investigation efforts as to the causes.

FBI also could not accurately identify all accountable assets because of improper controls related to its bar codes—a key tool for maintaining accountability and control over individual assets.[12] FBI relied on contractors to affix the bar codes, yet did not track the bar code numbers given to contractors, the bar code numbers they used, or the bar code numbers returned. Moreover, FBI provided incorrect instructions to contractors, initially directing them to bar code certain types of lower cost equipment that did not need to be tracked. FBI's loss of control over its bar codes and failure to timely enter assets into its property tracking system seriously hampered its ability to maintain accountability for its Trilogy equipment. Accountability for equipment was further undermined by FBI's failure to perform sufficient physical inventory procedures to ensure that all assets purchased with Trilogy funds were actually located during the physical inventory.

[12] The use of bar codes involves affixing a machine-readable bar code to a controlled item, which can then be scanned and compared to an equipment inventory listing as part of a periodic physical inventory.

Given the serious nature of these control weaknesses, we performed additional test work to determine whether all accountable assets purchased with Trilogy funds could be accounted for and found that FBI was unable to locate 1,404 of these assets. These were items such as desktop computers, laptops, printers, and servers. In written comments on a draft of our report, FBI told us that it had accounted for more than 1,000 of these items. During our agency comment period, FBI stated that it had found 237 items we previously identified as missing and provided us evidence, not made available during our audit, to sufficiently account for 199 of these items. We adjusted the missing assets listing in our report to reflect 1,205 (1,404 – 199) assets as still missing. FBI later informed us that the approximately 800 remaining items noted in its official agency response included (1) accountable assets not recorded in PMA because they were either incorrectly identified as nonaccountable assets or mistakenly omitted, (2) defective accountable assets that were never recorded in PMA and subsequently replaced, and (3) nonaccountable assets or components of accountable assets that were incorrectly bar coded.

We considered these same issues during our audit and attempted to determine their impact. For example, as stated in our report, FBI told us that components of some nonaccountable assets that were part of a larger accountable item may have been mistakenly bar coded. Using FBI guidance on accountable property, we determined that 103, or about 11 percent, of the 926 missing assets purchased by CSC may have represented nonaccountable components. Because FBI could not provide us with the location information, we could not definitively determine whether the items were accountable assets. During the course of our audit, FBI was not able to provide us with any evidence to support its other statements regarding the reasons the assets could not be located.

While we are encouraged by FBI's current efforts to account for these assets, its ability to definitively determine their existence has been compromised by the numerous control weaknesses identified in our report. Further, the fact that assets have not been properly accounted for to date means that they have been at risk of loss or misappropriation without detection since being delivered to FBI—in some cases, for several years.

Concluding Comments

FBI's Trilogy IT project spanned 4 years and the reported costs exceeded $500 million. Our review disclosed that there were serious internal control weaknesses in the process used by FBI and GSA to approve contractor charges related to Trilogy, which made up the majority of the total reported project cost. While our review focused specifically on the Trilogy program, the significance of the issues identified during our review may indicate more systemic contract and financial management problems at FBI and GSA, in particular when using cost-reimbursable type contracts and interagency contracting vehicles. These weaknesses resulted in the payment of millions of dollars of questionable contractor costs, which may have unnecessarily increased the overall cost of the project. Unless FBI strengthens its controls over contractor payments, its ability to properly control the costs of future projects involving contractors, including its new Sentinel project, will be seriously compromised. Further, weaknesses in FBI's controls over the equipment acquired for Trilogy resulted in millions of dollars in missing equipment and call into question FBI's ability to adequately safeguard its equipment, as well as confidential and sensitive information that could be accessed through that equipment from unauthorized use.

Our companion report includes 15 recommendations to help improve FBI's and GSA's controls over their invoice review and approval processes and to address questionable billing issues we identified. It also includes 12 recommendations to help improve FBI's accountability for assets. FBI concurred with our recommendations and outlined actions under way and further planned actions to address the weaknesses we identified. FBI also provided additional information related to Trilogy assets we identified as missing. While GSA accepted our recommendations, it did not believe that one of them was needed, and described some of the improvements to its internal controls and other business process changes already implemented. GSA also expressed concern with some of our observations and conclusions related to the invoice review and approval process and our analysis of airfare costs. We continue to believe that our report is accurate and that all recommendations should be implemented.

We understand that FBI has outlined actions to implement our recommendations. While we are encouraged by these efforts, let me just emphasize the importance of continually monitoring the implementation of corrective actions to ensure that they are effective in helping to avoid the types of control lapses that we identified throughout the Trilogy project. Without such vigilant monitoring, Sentinel and other efforts will be greatly exposed to similar questionable or inappropriate payments and lack of accountability over assets.

Mr. Chairman and members of the committee, this concludes my prepared statement. I would be pleased to answer any questions that you may have.

Contact and Acknowledgments

For more information regarding this testimony, please contact Linda M. Calbom at (202) 512-9508 or calboml@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this testimony. Individuals making key contributions to this testimony included Steven Haughton (Assistant Director), Ed Brown, Marcia Carlsen (Assistant Director), Lisa Crye, and Matt Wood. Numerous other individuals contributed to our audit and are listed in our companion report.

(Rev. 08-28-2000)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/29/2002

To: Pittsburgh

From: Pittsburgh
Squad 4
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]ro TRO

b6
b7C

Case ID #: ~~(S)~~ 199-0 (Pending)

Title: ~~(U)~~ IT Matters

Synopsis: ~~(U)~~ To report results of investigation of Pittsburgh anti-war activity.

~~(U)~~ **Derived From :** G-3
Declassify On: X1

Details: ~~(U)~~ The Thomas Merton Center (TMC), 5125 Penn Avenue, Pittsburgh, Pennsylvania, telephone: (412) 361-3022, webpage: www.thomasmertoncenter.org, is a left-wing organization advocating, among many political causes, pacificism.

~~(U)~~ TMC holds daily leaflet distribution activities in downtown Pittsburgh and is currently focused on its opposition to the potential war with Iraq. According to these leaflets, Iraq does not possess weapons of mass destruction and that, if the United States invades Iraq, Sadam Hussien [sic] will unleash bio-chemical weapons upon American soldiers.

~~(U)~~ TMC advertises its activities on its webpage. On November 24, 2002, TMC coordinated the 8th Annual An-Nass (Humanity) Day at the Islamic Center of Pittsburgh, 4100 Bigelow Blvd., Pittsburgh, Pennsylvania 15213. The contact person for this event was Farooq Hussaini of the Islamic Center, work telephone: (412) 622-8838, home telephone: [redacted] email: [redacted] URL: www.icp-pgh.org. The purpose of An-Nass Day was "to bring all people of Pittsburgh together in understanding and respecting each other and also to inform them about Islam and Muslims."

~~SECRET~~

b6
b7C

I:\4\[redacted]333TRO01.EC

DECLASSIFIED BY 60309AUCtam/dcg/mbh
ON 01-12-2006

199-0-734

SECRET

To: Pittsburgh From: Pittsburgh
Re: (S) 199-0, 11/29/2002

(S) Tim Vinning, the Merton Center's executive director, stated to Pittsburgh Tribune Review columnist Mike Seate that there are more than a few Muslims and people of Middle Eastern descent among the regulars attending meetings at the Merton Center's East Liberty headquarters.

(S) On November 29, 2002, SA [redacted] photographed TMC leaflet distributors at the Pavilion in Market Square, Pittsburgh, Pennsylvania. These photographs are being reviewed by Pittsburgh IT specialists. b6 b7C

(S) One female leaflet distributor, who appeared to be of Middle Eastern descent, inquired if SA [redacted] was an FBI Agent. No other TMC participants appeared to be of Middle Eastern descent. b6 b7C

♦♦

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

Pittsburgh, PA 15203-2148
February 26, 2003

INTERNATIONAL TERRORISM
MATTERS

Pittsburgh Division Joint Terrorism Task Force (JTTF) investigation has revealed the following information of which your agency may already be aware:

The Thomas Merton Center (TMC), located at 5125 Penn Avenue, Pittsburgh, Pennsylvania (PA), telephone 412-361-3022, webpage: www.thomasmertoncenter.org, has been determined to be an organization which is opposed to the United States' war with Iraq. A review of the above website revealed that when the United States begins war with Iraq:

> "All who desire peace and an end to war gather at the Federal Building downtown, corner of Liberty and Grant at 12 noon for an interfaith prayer vigil, 5 P.M. for a rally, and possible civil disobedience for those prepared to do this."

Also listed on the website is the date February 15, 2003. This day is a day of international protestors against the war promoted by United for Peace and Justice (www.unitedforpeace.org). The organization hosted the international rally and march against the war in New York City at the United Nations Building. Hundreds of people from the Pittsburgh region were making the trip to New York City for the protest. In addition, thousands more were anticipated in local marches, rallies, and vigils in Youngstown, Ohio (OH), Morgantown, West Virginia (WV), and Butler, Meadville, and Pittsburgh, PA.

Regional events included:

12:00 P.M. North Side Vigil for Peace in Iraq. Allegheny UU Church, North Avenue and Resaca Place (North Side)

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-04-2006 BY 60309AUCtam/dcg/mbh

INTERNATIONAL TERRORISM
MATTERS

12:00 P.M.	East End Community Stand for Peace, corner of Penn and Highland (East Liberty)
12:00 P.M.	Regent Square Community Vigil for Peace in Iraq. Waverly Church corner of Forbes and Braddock (Regent Square)

The above information is for your use and any action deemed appropriate.

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

May 2, 2006

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
May 2, 2006

Mr. Chairman, Senator Leahy, and members of the Committee on the Judiciary:

Thank you for inviting me to testify about the Office of the Inspector General's (OIG) oversight work related to the Federal Bureau of Investigation (FBI). As the FBI continues its transformation after the September 11 attacks, the OIG continues to devote extensive resources to examining FBI programs and operations. We have conducted many reviews in critical areas, including the FBI's efforts to upgrade its information technology systems (IT); its hiring, training, and retention of critical employees; its efforts to share information with its federal, state, and local law enforcement and intelligence partners; its allocation of investigative resources; its counterespionage and internal security challenges; and its management of the FBI laboratories. In addition, we continue to review allegations of civil rights and civil liberties abuses involving FBI and Department employees.

In this written statement, I first will make several general comments on the key challenges that the FBI continues to face. I will then describe in more detail reviews the OIG has conducted related to these issues. I base my general comments on the numerous FBI reviews conducted by the OIG, as well as my more than 11 years in the OIG reviewing FBI programs, the last 5½ during which I have served as the Inspector General.

When assessing the FBI, I believe it is important first to acknowledge the dedication and talent of its employees. The FBI attracts patriotic individuals who are committed to the FBI's important mission. These employees deserve recognition for the sacrifices they make in carrying out their critical responsibilities.

Their task is difficult, and the FBI is under regular and probing scrutiny by Congress, the OIG, and other oversight entities. That is as it should be. Given the importance of its mission and the impact the FBI has on safety, security, and civil rights in the United States, such scrutiny is warranted. But

I have found that its leaders, particularly Director Mueller, understand the value of such independent scrutiny.

In general, I believe the FBI has made some progress in addressing some of its critical challenges, but more progress is clearly needed. The first area where additional progress is needed is the ongoing effort to upgrade the FBI's information technology systems. For too long the FBI has not had the modern IT systems it needs to perform its mission as efficiently and effectively as it should. The FBI's IT systems must give its employees the ability to effectively analyze, share, and act on the vast amount of information the FBI collects. However, the FBI's failed Virtual Case File effort was a major setback – in both time and money – with regard to the FBI's urgent need for IT modernization.

While the FBI has made progress in other IT areas, as Director Mueller has pointed out in his written statement, the FBI still does not have a modern, effective case management and records system. As I discuss in more detail below, the OIG believes the FBI has learned painful and expensive lessons from its setbacks on the Virtual Case File as it works to develop a new case management system in the Sentinel project. As of now, Sentinel appears to be on the right track, although we have identified several important issues the FBI needs to address as it moves from pre-acquisition planning to development of the Sentinel system. The OIG plans to aggressively monitor the Sentinel project, and we will raise any additional concerns with the FBI and this Committee as the project moves forward.

A second challenge for the FBI is to aggressively pursue its law enforcement and intelligence-gathering missions while at the same time safeguarding civil rights. Pursuant to the OIG's responsibilities under Section 1001 of the Patriot Act, the OIG has investigated allegations of civil rights and civil liberties abuses, and we have also performed various reviews to assess whether the FBI is complying with guidelines that regulate its investigative activities. Examples of recent OIG reviews touching on civil rights and civil liberties include our review of the FBI's compliance with the Attorney General's investigative guidelines, our review of reports of possible intelligence violations forwarded to the President's Intelligence Oversight Board, and our review of the FBI's interviews of protesters connected to the 2004 Democratic and Republican National conventions. Currently, we are conducting other reviews relating to civil rights issues, including the FBI's use of National Security Letters and subpoenas for records under Section 215 of the Patriot Act.

A third critical challenge for the FBI is to recruit, train, and retain skilled individuals in its many critical occupations. The FBI has little difficulty attracting talented special agents. But its success in recruiting, training, and retaining individuals in other positions, such as intelligence analysts, linguists,

and technology positions, is mixed. Moreover, the FBI also has continuing challenges with turnover in key management positions at FBI Headquarters and in the field. In my view, rapid turnover in these critical positions reduces the FBI's effectiveness.

Fourth, in large part the FBI's success depends on its ability to share information, both internally within the FBI and externally with its federal, state, and local partners. The FBI is part of the larger intelligence and law enforcement community, and it must share and receive information from its partners in an effective and efficient manner. The ongoing challenge is to ensure that the right people have access to the right information. Without effective information sharing, the FBI's impact in its counterterrorism, counterintelligence, and criminal missions will be reduced.

Fifth, while there is little dispute that the FBI must transform itself to place counterterrorism as its highest priority, the FBI cannot neglect other investigative areas where it has a critical and unique role to play. In this regard, the OIG has conducted a series of reviews analyzing the FBI's allocation of investigative resources after the September 11 terrorist attacks. We have identified areas where the FBI has reduced its investigative efforts and where other federal, state, and local law enforcement agencies have been able to step into the gap. Yet, in other areas – such as financial institution fraud, telemarketing fraud, and drug cases outside metropolitan areas – we found that investigative gaps remain. We believe the FBI and the Congress need to continually monitor the FBI's allocation of resources to ensure that important investigative areas are not unduly affected by the FBI's reallocation of resources.

Sixth, as the Robert Hanssen case demonstrated so tragically, the FBI must remain vigilant in its internal security and counterespionage efforts. It would be folly for the FBI to believe that the Hanssen case was a unique event that is unlikely to ever occur again. After the Hanssen case, the OIG and the Webster Commission made numerous recommendations to improve the FBI's internal security. The OIG is now conducting a follow-up review to assess the FBI's progress in improving its internal security. Certainly, the FBI must balance security measures with the need to share information efficiently. But the FBI can never afford to become complacent about the continuing threat of espionage, from both inside and outside the FBI.

Seventh, the FBI is a leader in a variety of forensic science disciplines, and its Laboratory is world-renowned. But mistakes in the FBI Laboratory can have dramatic consequences, as demonstrated by the Laboratory's fingerprint misidentification in the Brandon Mayfield case. The Mayfield matter highlighted the fact that the FBI faces a continuing challenge to ensure the

reliability of its scientific methods. The OIG has performed various audits to monitor quality control issues in the Laboratory, including its DNA analysis and management of Combined DNA Index System (CODIS). The FBI must be vigilant to ensure that Laboratory is not vulnerable to mistakes or willful abuse.

Based on the many reviews of the FBI conducted by the OIG, I believe these issues represent some the most critical challenges confronting the FBI. In the remainder of this statement, I discuss OIG reviews in these general areas and describe in more detail what they found.

I. FBI INFORMATION TECHNOLOGY

Over the years, the OIG has reviewed and monitored the FBI's efforts to upgrade its information technology systems. The most recent effort is the FBI's Sentinel program, a project to replace the FBI's antiquated Automated Case Support (ACS) system with a modern case management system.

In March 2006, the OIG released the first in a series of audits that will monitor the FBI's development and implementation of the Sentinel project. Sentinel is the successor to the $170 million Virtual Case File project that the FBI ended unsuccessfully after 3 years. Reviews by the OIG found that the Virtual Case File project failed for a variety of reasons, including poorly defined and slowly evolving design requirements, weak information technology investment management practices, weaknesses in the way contractors were retained and overseen, the lack of management continuity at the FBI on information technology projects, unrealistic scheduling of tasks, and inadequate resolution of issues that warned of problems in project development.

In light of these issues, the OIG's March 2006 audit evaluated the FBI's progress on the Sentinel project. We assessed the FBI's pre-acquisition planning for Sentinel, including the approach, design, cost, funding sources, time frame, contracting vehicle, and oversight structure. The OIG found that the FBI has taken important steps to help prevent the types of problems encountered in the Virtual Case File project. In reviewing the management processes and controls the FBI has applied to the pre-acquisition phase of Sentinel, the OIG found that the FBI has developed information technology planning processes that, if implemented as designed, can help the FBI successfully complete Sentinel.

In particular, the OIG found that the FBI has made improvements in its ability to plan and manage a major IT project by establishing Information Technology Investment Management processes, developing a more mature

Enterprise Architecture, and establishing a Program Management Office dedicated to the Sentinel project.

However, the OIG identified several continuing concerns about the FBI's management of the Sentinel project: (1) the incomplete staffing of the Sentinel Program Management Office, (2) the FBI's ability to reprogram funds to complete the second phase of the project without jeopardizing its mission-critical operations, (3) Sentinel's ability to share information with external intelligence and law enforcement agencies and provide a common framework for other agencies' case management systems, (4) the lack of an established Earned Value Management process, (5) the FBI's ability to track and control Sentinel's costs, and (6) the lack of complete documentation required by the FBI's Information Technology Investment Management processes.

The OIG's prior reviews of the Trilogy IT project found that the FBI lacked an effective, reliable system to track and validate the project's costs. In our March 2006 review of Sentinel, we noted that although the FBI stated that it is evaluating a tool to track Sentinel project costs, potential weaknesses in cost control is a continuing project risk for Sentinel.

In addition, while the FBI has considered its internal needs in developing Sentinel's requirements, the OIG review expressed concerned that the FBI had not yet adequately examined or discussed Sentinel's ability to connect with external systems in other Department of Justice components, the Department of Homeland Security, and other intelligence community agencies. If such connectivity is not built into Sentinel's design, other agencies could be forced into costly and time-consuming modifications to their systems to allow information sharing with the Sentinel system.

The OIG will continue to monitor and periodically issue audit reports throughout the FBI's development of the Sentinel project in an effort to track the FBI's progress and identify any emerging concerns related to the cost, schedule, technical, and performance aspects of the project. Last week, the OIG initiated its second audit of the Sentinel project. This review will examine the $305 million contract recently announced with Lockheed Martin to determine, among other things, if the FBI has established the necessary work requirements, benchmarks, and other provisions to help ensure the success of the project.

II. CIVIL RIGHTS AND CIVIL LIBERTIES

In a recent speech, Director Mueller rightly stated that "As we recognize the necessity of intelligence gathering, we must also recognize the need to protect our civil rights. It has always been my belief, that in the end, we will be

judged not only on whether we win the war against terrorism, but also on how we protect the civil rights we cherish." During the past year, the OIG completed a series of reviews that either directly or indirectly examined the impact of FBI activities on civil rights and civil liberties issues.

1. Section 1001 Responsibilities: Section 1001 of the USA PATRIOT Act (Patriot Act) directs the OIG to undertake a series of actions related to claims of civil rights or civil liberties violations allegedly committed by Department of Justice (DOJ) employees. In March 2006, the OIG released its eighth semiannual report to Congress required by Section 1001. The report described the OIG's activities during the last 6 months related to civil rights and civil liberties complaints and the status of OIG and DOJ investigations of allegations of civil rights and civil liberties abuses by Department employees.

In addition to summarizing investigations and reviews undertaken by the OIG in furtherance of our Section 1001 responsibilities, the March Section 1001 report described the results of an OIG review of the FBI's reporting to the President's Intelligence Oversight Board (IOB) of possible intelligence violations. Our report detailed the types and percentages of violations reported by the FBI to the IOB in fiscal years (FY) 2004 and 2005, and the process used by the FBI to report such violations. Under the FBI's process, FBI employees self-report potential violations to the FBI's Office of the General Counsel, which reviews the possible violations to determine whether reporting to the IOB is required. Among the authorities the FBI used during this period that prompted reports to the IOB were the Foreign Intelligence Surveillance Act of 1978 (FISA), including FISA authorities that were expanded by the Patriot Act; the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection; and various statutory authorities used to issue National Security Letters to obtain information from third parties.

Examples of the violations that the FBI reported to the IOB in FYs 2004 and 2005 include FBI agents intercepting communications outside the scope of the order from the FISA Court; FBI agents continuing investigative activities after the authority for the specific activity expired; and third parties providing information that was not requested by the National Security Letter. Not all possible violations were attributable solely to FBI conduct. According to the data we reviewed, third parties such as telephone companies were involved in or responsible for the possible violations in approximately one-quarter of the cases in both years we examined. The OIG's Section 1001 report also provided detailed information that summarized the percentages of possible violations reported to the IOB, broken down by specific intelligence activity. We intend to continue to review these potential IOB violations and report on our findings in future reports.

2. FBI Interviews of Potential Protesters at the 2004 Democratic and Republican National Conventions: Last Friday, the OIG completed a review that examined the FBI's investigative activities concerning potential protesters at the 2004 Democratic and Republican national political conventions. The OIG initiated this investigation in response to reports that dozens of potential protesters had been interviewed prior to the conventions, including past protesters and their friends and family members, and that anarchist groups reported being "harassed" by federal agents.

The OIG review did not substantiate allegations that the FBI improperly targeted protesters for interviews in an effort to chill the exercise of their First Amendment rights at the 2004 Democratic and Republican national political conventions. The report concluded that the FBI's interviews of potential convention protesters and other related interviews, together with its related investigative activities, were conducted for legitimate law enforcement purposes and were based upon a variety of information related to possible bomb threats and other violent criminal activities.

The OIG found that nearly all of the FBI's protester-related investigative activity was devoted to addressing 17 distinct threats to the conventions falling within the FBI's domestic terrorism program. The nature of these threats varied. For example, in four cases the FBI received information indicating that persons who intended to demonstrate in Boston or New York also were planning on bombing sites at the conventions. The FBI also was made aware that a group with an extensive criminal history was known to be planning violent confrontations with police in one of the convention cities. In another matter, a convicted domestic terrorist was believed to be attempting to obtain a dangerous chemical, potentially for use against the police. The report concluded that the FBI addressed each threat in accordance with the Attorney General Guidelines, whether in the course of checking initial leads or conducting preliminary inquiries or full investigations.

In addition, the review identified seven terrorism enterprise investigations not initiated in connection with the 2004 conventions that generated convention-related criminal intelligence. As to these seven investigations, the OIG concluded that the investigative techniques utilized to obtain this intelligence were a logical outgrowth of the underlying investigations and that the investigative activity was undertaken in a manner consistent with the requirements of the General Crimes Guidelines.

3. The FBI's Compliance With Attorney General Investigative Guidelines: Since the Committee's last FBI oversight hearing, the OIG also completed its examination of the FBI's compliance with four sets of Attorney General Guidelines that govern the FBI's principal criminal investigative

authorities with respect to investigations of individuals and groups, and its use of confidential informants, its undercover operations, and its warrantless monitoring of verbal communications (also known as consensual monitoring). The Attorney General Guidelines provide guidance on the opening of FBI investigations, the permissible scope of investigations, and the law enforcement techniques the FBI may use. The Guidelines were last revised in May 2002.

In sum, while the OIG found many areas in which the FBI complied with the Attorney General Guidelines, the OIG also found significant non-compliance with the Guidelines governing the operation of confidential informants, failure to notify FBI Headquarters and DOJ officials of the initiation of certain criminal intelligence investigations, and failure to consistently obtain advance approval prior to the initiation of consensual monitoring.

Specifically, the OIG found one or more Guidelines violations in 87 percent of the confidential informant files we examined. The OIG review determined that required approvals for the use of informants were not always obtained, assessments designed to assess the suitability of individuals to serve or continue as confidential informants were not made or were incomplete, documentation of required instructions to informants were missing, descriptions of "otherwise illegal activity" by informants were not sufficient, and required notifications to FBI Headquarters or U.S. Attorneys' Offices were not made or documented. The OIG report noted that Guidelines violations can jeopardize DOJ prosecutions of criminals and also can lead to civil liability claims against the government.

The OIG review found, in contrast to the FBI's non-compliance with the Confidential Informant Guidelines, the FBI generally was compliant with the Undercover Guidelines, and the Headquarters unit supporting undercover operations was well managed and effective. The FBI also generally adhered to the provisions of the General Crimes Guidelines and the Consensual Monitoring Guidelines, although the OIG identified several deficiencies, particularly with regard to the Guidelines' requirements for supervisory authorization of the consensual monitoring.

The OIG report offered 47 recommendations designed to promote greater accountability for Guidelines violations by field supervisors; to use existing technology to track Guidelines violations; to enhance training on Guidelines requirements and the consequences of Guidelines violations to FBI investigations and DOJ prosecutions; to require supervisory approval and more systematic recordkeeping on the FBI's use of new authorities to visit public places and attend public events for the purpose of detecting and preventing terrorist activities; and to prepare a comprehensive implementation strategy for

the next Guidelines revisions. The FBI concurred with 43 of the 47 recommendations, and concurred partially with the 4 remaining recommendations.

4. Terrorism Screening Center: Within the past 11 months, the OIG completed two reviews examining various aspects 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 multiple 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.

As part of our reviews, the OIG examined the accuracy of the TSC's watchlists and the TSC process for correcting erroneous entries on the watch lists. The OIG concluded that the TSC had 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's June 2005 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.

Since issuance of the audit, the TSC has initiated a record-by-record review of the terrorist screening database to ensure accuracy, completeness, and consistency of the records. TSC staff informed the OIG it is focusing first on the records deemed most important. According to the TSC, review of the entire database, which contains more than 235,000 records, will take several years.

Ongoing reviews

5. FBI Observations of and Reports Regarding Detainee Treatment at Guantanamo Bay and other Military Facilities: The OIG currently is examining FBI employees' observations and actions regarding alleged abuse of detainees at Guantanamo Bay, Abu Ghraib, 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 military detention facilities. The questionnaire requested information on what the FBI employees observed, whether they reported observations of concern, and how those reports were handled.

6. The FBI's Use of Certain Patriot Act Authorities: As required by the *USA Patriot Improvement and Reauthorization Act* of 2005 (Reauthorization Act), the OIG is reviewing the FBI's use of two authorities amended by the Patriot Act: (1) the FBI's authority to issue National Security Letters to obtain certain categories of records from third parties, including telephone toll and transactional records, financial records, and consumer reports; and (2) the FBI's authority to obtain business records from third parties by applying for ex parte orders issued by the Foreign Intelligence Surveillance Court pursuant to Section 215 of the Patriot Act.

The Reauthorization Act directs the OIG to review the extent to which the FBI has used these authorities; any bureaucratic impediments to their use; how effective these authorities have been as investigative tools and in generating intelligence products; how the FBI collects, retains, analyzes, and disseminates information derived from these authorities; whether and how often the FBI provided information derived from these authorities to law enforcement entities for use in criminal proceedings; and whether there has been any improper or illegal use of these authorities. See Sections 106A and 119 of the Conference Report No. 109-333 (December 8, 2005). Our reviews, which we have recently begun, will include examination of FBI investigative files, interviews of FBI and other DOJ officials, and visits to FBI field offices.

7. Review of the Filiberto Ojeda Rios Shooting in Puerto Rico: At the request of the FBI Director, the OIG initiated an investigation of an FBI shooting incident in Puerto Rico that resulted in the death of Filiberto Ojeda Rios. Ojeda was a founder and leader of Los Macheteros, a pro-independence organization in Puerto Rico. Ojeda was arrested in 1985 in connection with a major bank robbery in Connecticut, but had been a fugitive since fleeing in 1990 while released on bail. During the FBI's attempt to arrest Ojeda at a rural residence in western Puerto Rico on September 23, 2005, an FBI agent was wounded and Ojeda was shot and killed. The OIG examined the circumstances surrounding the shooting and the FBI's entry into the residence, and we are in the process of drafting our report of investigation.

III. FBI HUMAN CAPITAL

The FBI faces continuing challenges to attract, train, and retain employees in some FBI positions, such as analysts, translators, IT specialists, scientists, and other support staff. Moreover, in various OIG reviews and investigations in the FBI, the OIG has witnessed significant turnover in supervisory employees. For example, the OIG's review of the FBI's Trilogy IT project found that the FBI had 15 different key IT managers, including 5 CIOs or acting CIOs and 10 individuals serving as project managers for various aspects of the project, which undermined the FBI's ability to successfully complete the Trilogy project. We also witnessed rapid turnover in important Headquarters and field supervisors' positions. As a recent NAPA report described, turnover in FBI leadership positions is extensive, with a median tenure of 15 months for Special Agents-in-Charge and 13 months for senior executives at Headquarters.

Reducing the turnover in key supervisory positions, and effective hiring, training, and retaining of FBI employees in key positions are some of the most important challenges facing the FBI. Without more stability, the FBI's effectiveness is diminished.

The OIG has conducted a series of reviews over the past several years that examine various aspects of this human capital issue. Two of those, with regard to intelligence analysts and linguists, are briefly discussed below.

1. Intelligence Analysts: In May 2005, the OIG issued an audit report that examined FBI efforts to hire, train, and retain intelligence analysts. After the September 11 terrorist attacks, the FBI focused on hiring, training, and retaining more fully qualified intelligence analysts. Yet, the OIG report found that while the FBI had made progress in hiring and training intelligence analysts, the FBI fell short of its hiring goals. Although the audit found that the analysts that the FBI hired generally were well qualified, the FBI has made slow progress toward developing a quality training curriculum for new analysts. The initial basic training course offered to analysts was not well attended and received negative evaluations, and the FBI replaced it with a revised 7-week training course.

FBI analysts who responded to an OIG survey indicated that generally they 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 5 years reported

dissatisfaction with their work assignments, compared to 13 percent of the analysts hired more than 5 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.

Last month, the OIG initiated a follow-up review to examine the progress made by the FBI since completion of our last review.

2. The FBI's Foreign Language Translation Program: The OIG also has examined the FBI's progress in improving its ability to translate foreign language materials. Two OIG reviews, issued in 2004 and 2005, found that the FBI's collection of material requiring translation had outpaced its translation capabilities, and the FBI could not translate all its foreign language counterterrorism and counterintelligence material. The audits also found that the FBI had difficulty in filling its need for additional linguists. The audits also concluded 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 for annual reviews of permanent and contract linguists.

IV. INFORMATION SHARING

The need for effective information sharing among intelligence and law enforcement entities has been a key finding of several national reviews convened after the September 11 terrorist attacks. Consequently, the OIG continues to review FBI's efforts to enhance information sharing and coordination with its law enforcement and intelligence partners. However, several reviews completed during the past year highlight the gaps that remain.

1. Seaport Security: Last month the OIG released an audit report that examined the FBI's efforts to protect U.S. seaports from terrorism. The United States has more than 360 seaports, and 95 percent of overseas trade flows through these ports or inland waterways, which often are located near major population centers. The protection of U.S. seaports is a shared responsibility among the Department of Homeland Security's (DHS) U.S. Coast Guard, the U.S. Customs and Border Protection, and the FBI. The Coast Guard protects and enforces laws at seaports while the Customs and Border Protection enforces import and export laws and inspects cargo at seaports. The FBI, as the lead federal agency for preventing and investigating terrorism, has an overarching role in protecting the nation's seaports, which includes gathering intelligence on maritime threats and maintaining well-prepared tactical capabilities to prevent or respond to maritime-based terrorism. Because of the number of different agencies involved with the nation's seaport security efforts, the issue of efficient and effective information sharing takes on vital importance.

The OIG review of the FBI's efforts to protect the nation's seaports found that since the September 11 attacks, the FBI has taken steps to enhance its capability to identify, prevent, and respond to terrorist attacks at seaports. For example, the FBI has created a centralized maritime security program at FBI Headquarters and, in addition to its counterterrorist tactical teams, has placed enhanced maritime SWAT teams in the FBI field offices closest to 14 of the nation's strategic seaports. Further, most of the FBI's 56 field offices have Maritime Liaison Agents responsible for coordinating with other federal agencies on maritime security.

However, we found that the FBI does not always assign these agents according to the threat and risk of a terrorist attack on a given seaport. For example, an FBI field office with six significant seaports in its territory has only one maritime liaison agent while another FBI field office with no strategic ports in its area has five maritime liaison agents.

Furthermore, the OIG review found that the FBI and the Coast Guard have not yet resolved issues regarding their overlapping responsibilities, jurisdictions, and capabilities to handle a maritime terrorism incident. We believe a lack of jurisdictional clarity could hinder the FBI's and the Coast Guard's ability to coordinate an effective response to a terrorist threat or incident in the maritime domain. Specifically, the report expressed concern about how confusion over authorities will affect the two agencies' ability to establish a clear and effective incident command structure in response to a terrorist attack on a seaport. In our judgment, unless such differences over roles and authorities are resolved, the response to a maritime incident could be confused and potentially disastrous.

The OIG report made 18 recommendations that focus on specific steps that the FBI should take to improve its counterterrorism efforts regarding seaport and maritime activities, including resolving overlapping responsibilities with the Coast Guard before a terrorist incident occurs; leading more interagency maritime-related exercises involving likely terrorism scenarios; preparing and using after-action reports after these exercises in order to identify lessons learned; and assessing the threat and risk of maritime terrorism compared to other threats and assigning resources accordingly.

2. Department of Justice Counterterrorism Task Forces: In a 2005 report, the OIG examined the operation of DOJ Counterterrorism task forces and assessed whether gaps, duplication, or overlap existed in the task forces' work. Three of 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. We also found that the FBI has not defined 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.

Ongoing reviews

3. Status of IDENT/IAFIS Integration: The OIG is completing a sixth review that examines efforts to integrate the federal government's law enforcement and immigration agencies' automated fingerprint identification databases. Our reviews concluded that fully integrating the automated fingerprint system operated by the FBI (IAFIS) and the system operated by the DHS (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 current OIG review is assessing the actions the FBI and DOJ have taken since the December 2004 report to achieve full interoperability of the FBI and DHS fingerprint systems.

4. Criminal Task Force Coordination: Another ongoing OIG review is examining, among other issues, information-sharing efforts among four DOJ task forces: the FBI's Safe Streets Task Forces, ATF's Violent Crime Impact Teams, the DEA's Mobile Enforcement Teams, and the USMS's Regional Fugitive Task Forces. In addition to assessing information sharing among the task forces, the review will evaluate whether investigations conducted by these DOJ task forces are well coordinated; whether they avoid duplication of effort; and whether they assist state, local, and tribal efforts to reduce crime.

V. ALLOCATION OF FBI INVESTIGATIVE RESOURCES

While the FBI has worked to transform itself after the September 11 attacks from a reactive law enforcement agency into an agency whose top priority is protecting the United States against terrorist attacks, the FBI maintains responsibilities for investigating criminal conduct. Given finite resources, striking an appropriate balance between its law enforcement and counterterrorism intelligence missions is a continuing challenge for the FBI.

The Effects of the FBI's Reprioritization Efforts: The OIG has issued several reviews that examined various aspects of the changes in the FBI's allocation of its investigative resources since the September 11 terrorist attacks. The most recent review, issued in September 2005, assessed 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 counterterrorism has affected other federal, state, and local law enforcement organizations. We determined that between FY 2000 and FY 2004, the FBI had formally reallocated 1,143 field agent positions away from investigating traditional criminal matters and placed these resources primarily in terrorism-related programs. In addition to the formal reallocation of positions, we found that the actual number of agents used to investigate criminal matters was significantly less than the FBI had allocated. The FBI actually utilized almost 2,200 fewer field agents to investigate these more traditional criminal matters in FY 2004 than it had in FY 2000. According to FBI officials, the additional agents were reassigned from criminal investigative areas to terrorism-related matters as needs arose.

The OIG review also found that the FBI opened 28,331 fewer criminal cases in FY 2004 than it had in FY 2000, a 45 percent reduction. Furthermore, we found that the FBI reduced the number of criminal-related

matters referred to U.S. Attorneys' Offices by 6,151, or 27 percent, between FYs 2000 and 2004.

Our interviews and surveys of federal, state, and local law enforcement officials regarding the impact of the FBI's changes in their jurisdictions found that, overall, the effects of the FBI's shift in priorities and resources on other law enforcement agencies' operations varied from agency to agency, and often from crime area to crime area. Most law enforcement agencies had not been significantly affected by the FBI's shift in investigative resources, although their caseloads had increased. But our review identified specific crime areas, such as financial institution fraud, in which other law enforcement officials said the FBI's reduced investigative activity has hurt their ability to address the crime problem in their area and has left an investigative gap. Our review also recommended that the FBI seek a more coordinated approach with other law enforcement agencies in certain investigative areas, including identity theft and human trafficking.

VI. FBI INTERNAL SECURITY

Ongoing Reviews

1. Follow-up Review of the FBI's Response to the Robert Hanssen Case: The espionage case of Robert Hanssen exposed long-standing problems with the FBI's internal security efforts. Hanssen was the most damaging spy in FBI history, and he betrayed some of this nation's most important counter-intelligence and military secrets, including the identities of dozens of human assets, at least three of whom were executed. The OIG review of the FBI's performance in detecting, deterring, and investigating the espionage activities of Hanssen was issued in August 2003. Our report concluded that Hanssen escaped detection for so long not because he was extraordinarily clever and crafty, but because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed internal security program. We found that there was little deterrence to espionage at the FBI, and the FBI's personnel and information security programs presented few obstacles to Hanssen's espionage.

We concluded that what was needed at the FBI is a wholesale change in mindset and approach to internal security. We recommended that the FBI recognize and take steps to account for the fact that FBI employees have committed espionage in the past and will likely do so in the future. We recommended that a unit at the FBI must be responsible for asking every day whether there is evidence that the FBI has been penetrated, and the FBI's internal security program must shift from a program relying on trust to a program based on deterrence and detection. We made 21 recommendations to

the FBI to improve its internal security and its ability to deter and detect espionage in its midst.

The OIG is now conducting a follow-up review to assess the FBI's progress in implementing the recommendations contained in the OIG's report on Hanssen.

2. The FBI's Handling of Chinese Intelligence Asset Katrina Leung: Another matter that exposed weaknesses in the FBI's handling of counterintelligence operations was the case of Katrina Leung, an asset in the FBI's Chinese counterintelligence program who had a long-term intimate relationship with her FBI handler, former Special Agent James J. Smith. At the request of the FBI Director, we are assessing the FBI's performance in connection with the handling of Leung. Our review is examining a variety of performance and management issues related to the FBI's handling of Leung, and whether there were problems in the way she was handled that the FBI should have acted upon sooner. The OIG is in the process of completing a classified report outlining the findings in this case. In addition, the OIG will attempt to create an unclassified executive summary of the report that can be publicly released.

VII. FBI LABORATORY

The FBI's forensic laboratories process a wide range of evidence ranging from DNA to firearms, and the work of the laboratories is critical to the successful investigation of a variety of crimes. Because of the increasing reliance law enforcement places on forensic laboratories, particularly DNA testing to solve crimes, and the increasing sophistication of the science involved, the OIG has focused on quality control and procedural issues in the FBI Laboratory to help ensure the reliability of its scientific methods and to guard against abuse.

1. FBI's Handling of the Brandon Mayfield Matter: In March 2006, the OIG released a 273-page report that examined the FBI's handling of the Brandon Mayfield case. Mayfield, a Portland, Oregon, attorney, was arrested by the FBI in May 2004 as a material witness after FBI Laboratory examiners identified Mayfield's fingerprint as matching a fingerprint found on a bag of detonators connected to the March 2004 terrorist attack on commuter trains in Madrid, Spain, that killed almost 200 people and injured more than 1,400 others. Mayfield was released 2 weeks later when the Spanish National Police identified an Algerian national as the source of the fingerprint on the bag. The FBI Laboratory subsequently withdrew its fingerprint identification of Mayfield.

We found several factors that caused the FBI's fingerprint misidentification. The unusual similarity between Mayfield's fingerprint and the fingerprint found on the bag confused three experienced FBI examiners and a court-appointed expert. However, we also found that FBI examiners committed errors in the examination procedure, and the misidentification could have been prevented through a more rigorous application of several principles of latent fingerprint identification. For example, the examiners placed excessive reliance on extremely tiny details in the latent fingerprint under circumstances that should have indicated that these features were not a reliable support for the identification. The examiners also overlooked or rationalized several important differences in appearance between the latent print and Mayfield's known fingerprint that should have precluded them from declaring an identification. In addition, we determined that the FBI missed an opportunity to catch its error when the Spanish National Police informed the FBI on April 13, 2004, that it had reached a "negative" conclusion with respect to matching the fingerprint on the bag with Mayfield's fingerprints.

2. DNA Reviews: Within the past 2 years, 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 addition, the OIG continues to audit 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. The OIG currently is analyzing findings from DNA laboratory audits – both OIG-conducted audits and external quality assurance audits – to determine if they reveal global trends and vulnerabilities. We also are assessing the adequacy of the FBI's administration of CODIS, including its oversight of the national DNA database, and evaluating its implementation of corrective actions in response to the original report.

VIII. CONCLUSION

In sum, while the FBI has made progress in addressing its changed priorities since the September 11 terrorist attacks, significant challenges and deficiencies remain, as various OIG reports have found. The FBI needs more improvement in critical areas such as upgrading its IT systems; balancing aggressive pursuit of its law enforcement and intelligence-gathering missions while safeguarding civil rights; hiring, training, and retaining skilled employees in a variety of critical occupations; sharing information effectively within and outside the FBI; monitoring its allocation of resources between its law enforcement and intelligence functions; maintaining vigorous internal security and counterespionage efforts; and ensuring the reliability of its scientific methods. These are not easy tasks, and they require constant attention and oversight. To assist in these challenges, the OIG will continue to attempt to conduct vigorous oversight of FBI programs and provide recommendations for improvement.

This concludes my prepared statement, and I would be pleased to answer any questions.

Statement
of
John C. Gannon
to the
United States Senate Committee on the Judiciary
Hearing on "FBI Oversight"
0930, 2 May 2006
Room 226 of the Dirksen Senate Office Building
Washington, D.C., 20510

Good morning, Mr. Chairman, and members of the committee. Thank you for the opportunity to participate in this important hearing on the FBI. I have great respect for the Bureau as a Federal law enforcement agency, and strong admiration for FBI officers with whom I have worked over the years. FBI officers are working hard today in the most challenging environment they have ever faced under an able Director of legendary energy, dedication, and integrity. They are not helped by outside carping. I am sensitive to this. But the debate about a domestic intelligence capability—analysis and collection—is important to our national security, and I believe the core of that debate should be public.

This written statement to the committee draws heavily on input I made to a recent Century Foundation task force. The views expressed are my own. They are shaped by my professional experience working with the FBI during a 24-year career at CIA, during a brief stint as the team leader for intelligence in the Transition Planning Office for the Department of Homeland Security (2002-2003), and during a two-year tour as the first Staff Director of the House Homeland Security Committee (2003 to 2005). They also are influenced my long experience building and managing analytic programs in the Intelligence Community, where I served as CIA's Deputy Director for Intelligence, as Chairman of the National Intelligence Council, and as Assistant Director for Analysis and Production.

I should point out that I have been working in the private sector for the past year, and have not had the close contact with the Bureau that I previously enjoyed. I concede that my perspective, therefore, is not as fresh on every point as I would like. In drafting this paper, I have opted for candor over caution and have some critical things to say. I do this as a former insider who is open to the charge that I could have done better at my series of jobs at CIA, the White House, and on the Hill. I accept this.

The salient fact is that, approaching five years after 9/11, we still do not have a domestic intelligence service that can collect effectively against the terrorist threat to the homeland or provide authoritative analysis of that threat. It is not enough to say these things take time. It could not be clearer from the Intelligence Community's experience over the past 25 years that it is extraordinarily difficult to blend the families of intelligence and law enforcement, and that the Bureau's organizational bias toward the latter—for deep-seated historic reasons--is powerful and persistent.

- Looking at where we are, we should be asking why it is so hard for the FBI to develop a national intelligence capability, and opening ourselves to the possibility that we have asked too much of an otherwise capable criminal-investigation agency. We should be looking seriously at other options.

- Looking at where we want to be, we also should be viewing domestic intelligence in the much broader context of US intelligence transformation, of the growing interlinkage of all our intelligence agencies, and of the globalization of intelligence and the threats that drive it. All this calls for unprecedented collaboration across US government agencies and a commitment to state-of-the art information technology--neither of which, in my experience, is a strong suit of the FBI.

I argued for some time after 9/11 that the FBI was the appropriate agency to develop a domestic intelligence capability, partly because of my aversion toward a new domestic intelligence agency, but even more because of what I clearly saw as the growing interconnectedness of intelligence and law enforcement, especially in combating transnational issues. I still have trouble letting go of that notion. But, watching the FBI struggle with its new national intelligence mandate and recalling earlier interagency "culture wars" in my career, I have changed my mind. I now doubt that the FBI, on its present course, can get there from here.

My view today can be encapsulated in the following six points:

- First, ***the FBI has made some progress on intelligence***. I distinguish between the Bureau's traditional law-enforcement mission and its new national intelligence mandate. In the first instance, I believe that the FBI is increasingly using intelligence collection and analysis, including in its new Field Intelligence Groups, against the increasingly complex issues associated with its criminal-investigation mission. The Bureau should be encouraged in this path--intelligence that benefits a Special Agent in Charge can also be useful at the national level.

- ***The FBI is unacceptably behind, however, in developing a national intelligence collection and analytic capability.*** The Bureau has not structured an intelligence collection requirements process that legitimate consumers can readily tap, and it is not, to my knowledge, producing, on any predictable basis, authoritative assessments of the terrorist threat to the homeland. These are serious gaps. It is a good thing that the Bureau's law-enforcement culture is being enriched by intelligence. It is not a good thing that law-enforcement continues to trump intelligence in the effort to build a domestic intelligence capability.

- Even if the FBI were doing better on this domestic intelligence mission, I believe we would find that **the mission in today's information environment is much bigger than the FBI, and well beyond its resources and competence to carry out**.

Domestic intelligence today is about protecting the US homeland from threats mostly of foreign origin. It does involve the FBI's law-enforcement and counterterrorism work, but it relates more to the establishment of a national intelligence capability integrating Federal, state, and local government, and when appropriate, the private sector in a secure collaborative network to stop our enemies before they act and to confront all those adversaries capable of using global electronic and human networks to attack our people, our physical and cyber infrastructure, and our space systems. These adversaries include WMD proliferators, terrorists, organized criminals, narcotics traffickers, human traffickers, and countries big and small—working alone or in combination against US interests. I see the FBI, on its present course, as a contributor to this vital effort—but not as the leader of a new model of collaborative effort in the information age. .

- ***Domestic intelligence, moreover, should be viewed as an integral part of US Intelligence Community reform.*** The connection between foreign and domestic intelligence must be seamless today because the threats we face know no borders. The challenge is government wide, has historic roots that long precede 9/11, and must be concerned, as I have suggested, with a range of deadly threats to our national security largely from abroad and not restricted to international terrorism. The domestic piece must be an essential part of the transformation of US intelligence driven by the Directory of National Intelligence (DNI), the Secretary of Defense, the Attorney General, and the Secretary of homeland Security. That coordinated effort today—which, in my view, needs stronger, sustained direction from the White House and the Congress--should be moving, as a top priority, to unify strategies, to clarify roles and responsibilities across competing agencies, and to reduce the IC's bloated bureaucracy—which is today larger than ever.

- ***The status quo is unacceptable.*** The two courses I suggest to get us moving forward, neither an easy fix, would require some shift of Federal Government resources and authorities and strong leadership from the Executive and Legislative branches.

    - ***First, if the FBI is to remain the agency of choice in developing a domestic intelligence capability, it will need much stronger and clearer direction and much closer oversight from the Executive and Legislative branches on the much bigger and faster structural steps it needs to take. The urgent objective must be to develop an intelligence capability that is not subordinated to the Bureau's criminal investigation mission and that is based on a level of collaboration—including with non-government experts--unprecedented in FBI history.*** I will not say that it cannot be done, but the evidence to date suggests otherwise.

    - The second suggestion, which takes some explaining, is to give the lead on domestic intelligence to ***a resuscitated and revitalized Department of Homeland Security (DHS)*** with the resources and authorities that the Homeland Security Act of 2002 intended—but were never provided. That Act, I believe, rightly recognized that the domestic intelligence mission

requires a new collaborative model, not just new rules for old games among legacy agencies. DHS's small and under-resourced Office of Intelligence is, by design, a collaborative enterprise involving multiple Federal, state, and local agencies. DHS itself has the mandate for outreach to the private sector and to non-government sources of information and expertise—which is made easier because the larger Department is neither a law-enforcement nor an intelligence agency. Conceptually, I believe DHS could succeed as the coordinator of domestic intelligence. And its prospects for success would increase significantly if the Department established regional organizations across the country—which are essential to the collaborative model I describe. ***But this will never happen unless the White House and Congress, altering their current posture, push hard for it.***

- Finally, ***I would argue strongly against the creation of a new, stand-alone domestic intelligence agency.*** When asked why we have not had a terrorist attack on US soil since 9.11, I give three reasons. First, the President's early decision to go after the terrorists wherever they could be found in the world weakened their capabilities and served as a powerful disincentive to strike us again. Second, the preventative and protective security measures taken by our Federal, state, and local governments—coordinated and not—have made it harder for terrorists to operate here. And, third, I believe that the hard-won Constitutional freedoms enjoyed by Americans, along with our unparalleled commitment to civil liberties embedded in law, work against the development of domestic terrorist networks that could be exploited by foreigners. In this context, America stands in marked and magnificent contrast to many of the regimes I covered daily and experienced on the ground as a CIA analyst. When I think through the implications of a nation-wide domestic intelligence service under the control of the Executive Branch, I conclude that it is neither needed nor desirable in our society. At best, the proposal is premature.

The Changing Threat

Today, the threat to the US homeland is global in nature and our response must integrate foreign and domestic intelligence as never before. Al Qaeda's attacks in New York, Pennsylvania, and Washington on 9/11 revealed that Osama bin Laden had developed-- below the radar of US intelligence--a human and electronic network across some sixty countries, spanning from the pre-modern world of Afghanistan to the post-modern world of Europe and the United States. Al Qaeda's flat network defeated a vast US government hierarchy that was not networked, including both our foreign and domestic intelligence agencies. The terrorists knew more about our world, and how to train and operate in it, than we did about theirs—the classic recipe for an intelligence failure. By any reckoning, the US government was not prepared to protect its people, not only against international terrorism but against the potential exploitation by any of our adversaries of global, IT-driven networks.

Domestic intelligence today must be global in perspective, collaborative to the core, and thoroughly networked to bring together the most reliable information, the best expertise, and the most advanced capabilities—in real time—to deal with today's dynamic, distributed, and dangerous threat environment. It must have state-of-the-art, multi-level-security communications to support a broad range of activities from assisting a big-city police officer to pursue sketchy intelligence leads in a gritty subway to helping expert analysts to track potential cyber attacks in a chrome-plated, plasma-screened national center. Domestic intelligence, in this context, should be seen as a critical element of the US Government's long-term transformation driven by the geopolitical and technological revolutions of the post-Cold War period.

Antecedents

The domestic intelligence challenge is not new, a critical point that both the 9/11 Commission and the WMD Commission missed in their failure to provide balanced historical perspective. The challenge long predates 9/11. It relates to the three distinct but intersecting revolutions faced by the Intelligence Community-- including the FBI-- over the past twenty years, which have encouraged trends that continue today. I focus briefly on this because I believe these revolutions, with or without 9/11, demand dramatically new and different models for US intelligence—not legacy makeovers.

The first revolution was geopolitical. It swept away the Soviet Union, transformed the face of Europe, and forced the Intelligence Community to confront a new, dispersed global threat environment in which non-state actors, including conventional and cyber terrorists, narcotics traffickers, and organized criminals, operated against US interests across national borders, including our own. The second revolution involves technology, primarily information technology, but also the rapidly advancing biological sciences, nanotechnology, and the material sciences—all bearing good news and "dual-use" bad news for America and mankind. The third revolution relates to homeland security. This is not just about the alarming proximity of the threat, but even more about the new national security stakeholders it brought to the fore, "first-responders" with a legitimate need and justifiable demand for intelligence support.

The IC, the policy community, and the Congress actually began to respond to this new, distributed threat environment in the mid 1980s, with the pace picking up dramatically in the ensuing decade. The FBI was involved at every turn. The DCI established the Counterterrorism Center (CTC) at CIA in 1986, followed thereafter by the Counternarcotics Center and several iterations of a counter-proliferation center—all mandated to focus collection, integrate analysis, and promote information sharing. Both CIA and DIA reorganized their intelligence units to meet new threats and enable technology in the mid 1990s. The FBI took similar steps later in the decade. The White House in 1998 established the position of National Coordinator for Security, Infrastructure Protection, and Counterterrorism.

Advancing technology drove the controversial creation of the National Imagery and Mapping Agency (NIMA) in 1996. NIMA(later named National Geospatial-

Intelligence Agency—NGA) launched a major push to get ahead of the geospatial technology curve, while the National Security Agency (NSA) began a fundamental transformation to adapt to the global revolution in communications technology. In 1998, the Ballistic Missile Commission, headed by Donald Rumsfeld, included with its report a "sideletter" critiquing IC analytic performance that was an impressive blueprint for reform. The FBI significantly increased its overseas presence and, prodded by the Webster Commission, developed a five-year strategic plan in the late 1990s that included goals to develop a comprehensive intelligence collection and analytic capability. Late in the decade, it established separate counterterrorism and counterintelligence centers.

The point I want to emphasize is that the FBI, as I observed it first hand, was acutely aware of an intelligence world turning upside down. It was closely involved in the establishment of the IC centers. DCI William Webster came from the FBI to CIA in 1987, where he issued a forward-looking –and, I believe, historic--directive that prohibited analysts who were directly supporting operations from providing the authoritative assessment on the impact of such operations. FBI leaders persuasively argued for the development of analytic capability in the Bureau during a strategic planning process in the late 1990s about the same time FBI launched its counterterrorism and counterintelligence divisions. The FBI also participated with IC analytic units in the work of the Community-side National Intelligence Producers Board, which did a baseline assessment of IC analytic capabilities and followed it up early in 2001 with a strategic investment plan for IC analysis.

The investment plan flagged to Congress the alarming decline in investment in analysis across the Community and the urgent need to build or strengthen interagency training, database interoperability, IC collaborative networks, a system for issue prioritization, links to outside experts, and an effective open-source strategy. The consensus, which included FBI, was strong that the IC needed to transform, and it was transforming—but neither fast enough nor in alignment with the unfocused and fast-changing priorities of the White House and Congress.

The FBI's leadership, as I saw it, was committed to transformation but its commitment seemed to flag over time. Its early post-war determination to share information and push the "wall" on information sharing between intelligence and law enforcement was set back by the sensational Ames, Nicholson, and Hanson espionage cases. And, to a large extent, I understood and accepted the reasons for this. In the larger culture war, however, I believe that change agents simply lost out to classic agents who successfully resisted reform to Bureau policies and practices. The need to transform against a new threat environment was well recognized, but the goal of establishing a distinct intelligence career service for analysts and collectors, with their own budgets and chains of command, did not get off the ground. To enhance collaboration, a small handful of Terrorism Task Forces (JTTFs) in the early 1990s grew to over 120 today, but I heard complaints that they, with some notable exceptions, were inadequate because they" served up" in the Federal bureaucracy much better than "down" into vulnerable localities where vital intelligence needed to be collected.

Pre 9/11 Trends

Four trends were clear as the IC entered the twenty-first century, and they all appear irreversible today. In one way or the other, they relate to America's current efforts to reform its intelligence services and to the particular challenge of domestic intelligence.

First, agencies were beginning seriously to respond to the ***growing impact of globalization.*** Globalization—the interconnectedness of networks moving information, culture, technology, capital, goods, and services with unprecedented speed and efficiency around the world and across the homeland—came to be seen not as a passing phenomenon but as the defining reality of our age. In a shrinking world of communications, foreign and domestic intelligence know no borders. This is not to say the whole Community wholeheartedly embraced technology to enable transformation nor that the White House or Congress made this a priority. But the direction was set. And the glaring technological shortcomings of HUMINT collection, the FBI, and local law enforcement came into sharp relief.

Second, pressures within the IC increasingly were toward ***decentralization***, not the centralized, "one-stop-shopping" models—including some ambitious interpretations of the National Counterintelligence Center (NCTC)--generally favored by Washington. The demand grew among diplomats and "warfighters" for a distributed model of collection management and analysis, because they were dealing increasingly with diverse transnational threats close to their locations. And they were aware that technology existed to reduce dramatically the "distance" between the producers and users of intelligence Combatant commanders, often playing the diplomat's role, demanded real-time intelligence support and insisted that they have their own analysts in place. While Federal agencies moved slowly and the FBI lagged behind, the defense community accelerated its transformation with the same determination that would later be shown after 9/11 by homeland "first responders."

-- Third, ***DoD, in this environment, gained increasing influence in IC forums and debates, including on budget priorities.*** The Congress in the late 1990s created the positions of Deputy Director of Central Intelligence for Community Management (DDCI-CM), and assistant directors of collection and analysis and production, all of which were resisted by CIA and inexplicably underutilized by the DCI to run an increasingly complex Intelligence Community. By sharp contrast, the Secretary of Defense successfully lobbied, against surprisingly little IC resistance, for the creation of an Undersecretary of Defense for Intelligence position, which was approved in 2002, adding more heft to what already was the IC's thousand pound gorilla. Significantly, the defense community got out ahead of the national community in calling for—and developing—both centralized and decentralized networks that would bring analysis and collection capabilities closer to military personnel on the front lines. The DoD turf grab further wounded a weakened CIA and eventually raised concerns about military involvement in

domestic intelligence, but it also responded to real, unmet defense community requirements for improved analysis and collection management.

--Fourth, blue-ribbon commissions in the late 1990s, as well as the IC's own strategic work, recognized the ***growing need for a homeland security strategy***, including for domestic intelligence, against catastrophic threats from terrorism, WMD proliferation, and cyberspace. It also stressed the vital role of the private sector as a source of critical information and solutions to hard security problems. Serious worries about the state of US homeland security long predated 9/11. In 1996, the Critical Infrastructure Commission pointed out how vulnerable we were to attack, and the Bremer, Gilmore, and Hart-Rudman Commissions were eloquent well before 9/11 in flagging our lack of preparedness for a terrorist attack—including the glaring shortcomings of both foreign and domestic intelligence.

What have we done since 9/11?

Since 9/11, we have created a large Department of Homeland Security; a Terrorist Threat Integration Center, later transformed into a more muscular National Counterterrorism Center; an FBI Directorate of Intelligence to staff and train analysts, an FBI National Security Program integrating the Bureau's three intelligence divisions, a Bureau-controlled Terrorist Screening Center to integrate terrorist watch lists; and a Director of National Intelligence to restructure the IC—an impressive array of new organizations. We have done more to protect our airspace, ports, and borders than at any time since World War II, though, in the absence of strategy, we have struggled to establish priorities—as Hurricane Katrina revealed-- and to discipline spending. State and local governments have improved their security sometimes on a regional level, often in unprecedented collaboration across jurisdictions. On the offensive, we successfully pursued terrorists relentlessly at home and abroad, which is arguably a major reason why we have not had another attack to the homeland. The importance of these hard-won achievements should not be diminished

But in a period of extensive government restructuring, we have not—nor could we have--hit the intended target every time. Small things have been neglected forgivably in an overly ambitious agenda, and so have some big things like adequately resourced programs for cybersecurity, biosecurity, critical infrastructure protection, government-wide information sharing, and domestic intelligence. And sometimes both the Administration and Congress have missed critical targets by a long shot, as Hurricane Katrina revealed in the fall of 2005. In New Orleans, DHS failed on its fundamental commitment—which I now believe exaggerated its potential from the get-go-- to coordinate Federal, State, and local preparedness. And the Congress, in a bloated 2005 Transportation bill larded with pork, completely missed the glaring infrastructure vulnerabilities in the Gulf. Before Katrina, we knew we were not where we should be in protecting America. Katrina showed we were much worse off than we thought.

Since I am prepared to argue that DHS could be the hub of a collaborative domestic intelligence service, I need to explain why the Department has been such a disappointment thus far. DHS, whatever its shortcomings, was the first answer of the Administration and Congress to the question of how to construct an overarching structure to integrate and focus government on homeland security. The Homeland Security Act of 2002 positioned DHS to play a leading role in enhancing US counterterrorism capabilities and in establishing the architecture for domestic intelligence. While not collecting intelligence, DHS would fuse terrorism-related intelligence from all sources in its mission to integrate foreign and domestic analysis of the terrorist threat. It would provide threat information to the twenty-two agencies integrated into the Department; to state and local governments; and, when appropriate, to the private sector. It would collect actionable information from them, and would produce integrated threat analysis to help prioritize the protection of America's critical infrastructure. It would be a key leader in promoting information sharing across the US Government. It would be the Federal coordinator of critically needed programs to address the threats of cyber- and bio-terrorism.

The core mission of DHS was to develop new capabilities to prevent another catastrophic attack on the homeland, to prioritize the protection of our critical infrastructure, and to improve our national—Federal, state, and local government—response if an attack should occur. Making America safer through new capabilities took precedence over the merger-and-acquisition questions related to standing up a 180,000-member department in the largest US Government restructuring in half a century. FBI would collect intelligence within the homeland, while the Department would be the primary integrator of intelligence from all sources and the primary analyzer of the terrorist threat to the homeland. It would also serve the IC, President, and the Congress as an indispensable evaluator—an upscale "team B"--of all intelligence inputs into its terrorism threat analysis. The DHS intelligence organization would compete with other agencies in senior expertise, not in numbers. With a broad information-sharing mission well beyond intelligence, it would be uniquely positioned to collaborate with non-government experts anywhere in the world.

While the design may have been imperfect, the execution was surely flawed. DHS stumbled from the start and, after three years of trying, has not achieved compliance with the Homeland Security Act. Congressional oversight has been uneven and largely unfocused. Both House and Senate committees, including the intelligence overseers, generally have fought harder to strengthen their own fractured jurisdiction than to coordinate a constructive approach to DHS and its vital national security mission.

We now have abundant data to assess DHS's and the IC's performance since 9/11. These include multiple Congressional hearings and investigations, reports from the the Office of management and Budget, the General Accountability Office, the Congressional Budget Office, the Congressional Research Staff, various Inspectors General, think tanks of every political persuasion, and the media with its growing access to former Administration officials. The IC story is disappointing but still with hope under the DNI. For DHS, it is largely a chronicle of a few victories made hard to achieve and many failures that should have been avoided.

President Bush's surprising announcement in his January 2003 State of the Union address of the creation the Terrorism Threat Integration Center (TTIC) was a well-intentioned and legally defensible initiative to promote sensitive intelligence sharing among key intelligence agencies. And it had immediate political appeal, including among leading Democrats as well as Republicans in the Congress. But it also was an alarming rejection of an urgently needed, overarching model for interagency collaboration that would not be easily replaced—and, in fact, never was. In resource terms, it was a body blow to the not-yet-functioning DHS, which had just been given comparable responsibilities for fusing intelligence and integrating foreign and domestic analysis under the freshly minted Homeland Security Act. Agencies that had committed to provide detailees to the fledgling Department backed off to husband scarce resources. Congress was surprised and confused and found many other reasons to be disappointed by White House restraints on the Department, especially its reluctance to provide DHS's intelligence component with the facilities, infrastructure, connectivity, and personnel it need to do its job. But, with some exceptions, its own oversight rarely approached a rigorous standard.

Since 9/11, Congress has consistently favored creating new "boxes" rather than fixing or eliminating the old ones—without seriously assessing the cost to existing critical programs. Structure itself, in my experience in the IC, is rarely either the cause or the remedy for performance problems. In the effort to stand up new structures after 9/11, Congress did not baseline existing IC resources. It created new centers while pulsing up rather than consolidating old ones It unintentionally encouraged the stretching of scarce analytic resources literally to the breaking point, the dispersal of valuable expertise, and an unprecedented reliance on the contracting community for analytic staffing, workforce management, and training. When I left the Hill over a year ago, a significant majority of the analysts assigned to the NCTC—our new gold standard in counterterrorism--were contractors.

The expansion, as I saw it first hand, increased production while reducing authoritative analysis—or quality control—across these units. This has produced the first generation of intelligence analysts without adequate numbers of experienced managers to train them. I once argued, and the intelligence oversight committees agreed, that it takes the better part of a decade to bring a new IC analyst to peak performance. Today, the majority of analysts in many units have less than five years experience.

While the current situation is correctable, Post-9-11 restructuring has divided—not concentrated—accountability for threat assessments across a larger number of analytic units at CIA, FBI, DHS, and NCTC. It has confused civilian and military roles and raised alarms about military involvement domestic intelligence in the emergence the powerful and effective Northern Command, in the expansion of DoD's Counterintelligence Field Activity (CIFA) that protects US military facilities, and in NSA's "warrentless" surveillance of US citizens' communications. FBI has fallen short in developing analytic and collection capabilities, and DHS is way behind in building the necessary relationship with the private sector to counter serious and growing threats from

cyber- and bioterrorists. If the FBI were to be placed in the IC penalty box, it would have plenty of company.

Our record since 9/11, then, is a mixture of notable successes, commendable but stalled efforts, and significant failures Much of what we have done has been understandably reactive and uncoordinated—often resulting from conflicting priorities and unfocused interplay of the Executive and Legislative branches in an atmosphere of crisis. Current approaches, as a whole, are not cost effective as a blueprint for the future. America needs a comprehensive strategy for national security—including homeland security and domestic intelligence—and bold leadership to implement it.

What do we need to do?

The hastily drafted Intelligence Reform and Terrorism Prevention Act of 2004 created opportunities but no guarantees for enhancing our national security, and it left a lot of holes that only smart leaders can fill. In moving forward, the Executive Branch, in close collaboration with Congressional Committees of jurisdiction, needs to develop a strategic reform agenda with clear reform goals and metrics. We should see this not as an option on a healthy progression on homeland security and intelligence reform but as an imperative on a troubled journey in which too many opportunities have been missed and too many mistakes have been made—and not admitted let alone addressed. And there is nothing self-correcting about many of the alarming trends we observe today.

It is normally a feckless exercise to recommend that a President take direct charge of a government program. But Intelligence transformation, in my view, is not simply another government program. It is the epic mission of our generation, with major implications for the future security of our country. As matters stand today, the President's leadership will be essential to get the government on the right course and to reverse the effects of high-level bureaucratic gamesmanship and, in some cases, failed, unaccountable leadership at lower levels. What follows are my own recommendations intended to help focus a needed debate. I know well that I am open to challenge. And, I am glad to say, on several issues, my mind can be changed.

Recommendation 1-- ***Restore Accountability***: The President should establish by executive order an Intelligence Transformation Group (ITG)—or its functional equivalent--of the National Security Council, chaired by the President with delegation to the National Security Adviser, to include the Secretary of Defense, the Secretary of Homeland Security, the Attorney General, and the DNI. The mandate should be to develop and implement a strategic plan for IC reform, based on agreed-upon priorities consistent with the Intelligence Reform and Terrorism Prevention Act of 2004, led by the President in close collaboration with the major agencies affected. The organization need not be so formal, if the President so chooses, but his strong hand must be evident in making relevant agency heads responsible and accountable for implementation of his agenda and for presenting a unified front in dealing with the Congress.

Recommendation 2—*Resist Structural Buildup:* The Administration and the Congress need to restrain their longstanding tendency to adopt structural solutions to functional problems. It is politically more difficult to make leadership accountable for fixing existing organizations, including streamlining them, but it is ultimately less costly and more effective in implementing real reform. In any restructuring, we need to balance better than we have the competing needs for centralized and decentralized models for analysis and collection. The hasty establishment of the TTIC and NCTC taught us that the resistance encountered to these centralized models was in part the result of legitimate leadership concern about degrading critical capabilities needed in an increasingly decentralized Intelligence Community. Structure, by itself, is no panacea.

- *Whatever the merits that some see to a new, stand-alone domestic intelligence service (including on the UK or Canadian models), the proposal is premature. I believe it is a bad idea in the first place. If adopted, however, the original vision of its proponents would likely be significantly altered in the counterproductive interplay between the Administration and the Congress. The journey would be painful and protracted, and the destination would not be what its proponents planned, which was surely the case with DHS.*

Recommendation 3—*Strengthen DHS and Give it an Overarching Domestic Intelligence Role* The President should publicly, as well as in his leadership of the ITG, make clear his support for a strong DHS--with the capabilities the Homeland Security Act intended--to coordinate the programs and prioritize the activities of Federal, state, and local governments to prevent man-made (e.g. terrorism) and natural disasters, to protect our people and critical infrastructure, and to respond effectively if such disasters should occur. DHS was designed in statute to be an independent agency to nurture new capabilities to protect America against information-age threats. If properly resourced and supported by the White House, it would be well positioned to be America's focal point for domestic intelligence.

Recommendation 4—*Establish DHS Domestic Regions*: The DHS second-phase review should be revised to give the Secretary responsibility for assuring a two-way intelligence exchange with state and local governments—as well as with the 22 agencies incorporated into DHS. As a matter of priority, it should call for the development of strong regional organizations—indispensable to a national intelligence system as well as to effective DHS preparedness and response--to help fulfill this mission.

- *While the Federal Government in recent years has fallen short in delivering threat-based information to enable state and local governments and the private sector to prioritize critical infrastructure protection, regions around the country have taken impressive steps largely on their own to improve their counterterrorism capabilities across jurisdictions. Obvious examples are New York City (with Northern New Jersey), the*

District of Columbia (with Baltimore and Richmond), Miami, Houston, Los-Angeles-Long Beach, Seattle-Tacoma, Chicago, and Detroit.

- *These regions should have unfettered access to all Federal intelligence agencies, not just the FBI or the NCTC. The Federal Government has protested that it cannot grant security clearances to 13,000 police departments across the country. But it can clear selected officials in these eight regions as a start toward a reliable and sustainable national intelligence system.*

Recommendation 5—*Clarify FBI's Particular Role in Domestic Intelligence*: The FBI, its fifty-six field stations, and its growing network of over 120 Joint Terrorism Task Forces (JTTFs) have a part to play in the development of a national intelligence capability but, as we have argued, it should be a collaborative, not a leading role. We should, once and for all, lower expectations of a dominant role for the Bureau in domestic intelligence. The FBI, unless the White House and Congress are prepared to push a fundamental FBI restructuring in favor of intelligence, should not be expected to produce either the authoritative analysis of the terrorist threat to the homeland or a national collection requirements system. The President and the ITG should make FBI accountable only for developing an intelligence collection system to support law enforcement and a limited analytic capability in collaboration with state and local governments—both of which the Bureau is pursuing now.

Recommendation 6: *Clarify Departmental Roles and Responsibilities:* The President and the ITG should work urgently to clarify roles and responsibilities of key agencies with responsibilities for intelligence and homeland security missions. The NCTC, DHS, DoD (especially the Northern Command), CIA, and FBI, while understandably enlarging their missions, are bumping into each other in the integration of foreign and domestic intelligence, and colliding in establishing working relationships with state and local governments. This is a manageable problem if caught early, a serious issue with implications for preparedness, response, and civil liberties if ignored. Recent press reports of military involvement in domestic intelligence collection may or may not turn out to be serious concerns for the protection of civil liberties. They are, however, clear indications of a Federal Government and Congress that have failed to clarify roles and responsibilities in a new threat environment.

Recommendation 7—*Promote Government-wide Information Sharing*: This goes to the heart of reform that will enable us to fight tomorrow's war, not yesterday's. The Program Director for Information Sharing, a position given government-wide authorities by statute, should be placed preferably in the National Security Council or otherwise in an invigorated DHS, not under the DNI where the White House recently has placed it at least partly on the misguided recommendation of the WMD Commission. The effect of the White House action, which will be felt across the Federal Government as well as in a jurisdiction-focused Congress, will be to foster the backward-looking impression that information sharing is just an intelligence issue. It also will take pressure off other agencies—including the Department of Justice—to play seriously in this top-

priority effort, and it will guarantee the perpetuation of "legacy" behavior over the long term. It lessons the probability that an effective, government-wide information-sharing network, such as the Markle Trusted Network, will be implemented any time soon.

Recommendation 8—*Back the DNI, but Hold Him Accountable:* The President and the ITG should actively support and carefully monitor the implementation of the DNI's agenda to reform IC management, to professionalize the intelligence service, and to improve intelligence collection and analysis. The DNI's agenda should include priorities of common concern to DoD, DHS, and the Attorney General: improving HUMINT capabilities to steal secrets (with less public exposure), enhancing technical collection, and open-source capabilities; upgrading analysis (with greater outside exposure); establishing a cross-agency program evaluation capability; developing interagency professional and technical training programs in a National Intelligence University; building a user-friendly collection management system capable of responding to real-time requirements in the field as well as in Washington; and forging enduring relationships with outside experts, especially with the global scientific community. The high expectations on the DNI, of course, will only be realized if he has the backing of the White House.

Recommendation 9—*Clarify CIA's Role Under the DNI:* The advent of the DNI has ruptured CIA's 57-year special relationship with the President. CIA analysts and HUMINT officers were directly responsible through their Director to the President as IC coordinators rather than to a cabinet-level policymaker. The recent placement in CIA of the new National HUMINT Service, with IC-wide coordinating responsibilities, is a good step. The Agency's unique analytic capabilities need to be recognized and fostered in a similar fashion. They are an invaluable asset to the DNI and the President that should not be squandered.

Recommendation 10—*Push Congressional Reform:* The Executive Branch should continue to press for the reform of Congressional jurisdiction. The 9/11 Commission rendered a serious and damning critique of Congressional oversight. Both the House and Senate have commendably created committees to consolidate some of the far-flung jurisdiction on homeland security, though jurisdiction still is scattered over multiple committees and subcommittees. None of this, moreover, has changed the inadequate oversight of the intelligence agencies or otherwise gone far enough to align, in any lasting way, Executive and Legislative branch priorities for IC reform. Reform of Congressional oversight will be a continuous work in progress for the indefinite future. Improving our intelligence capabilities is today an imperative, not an option, if we are to confront the complicated, globally distributed, and increasingly lethal national-security threats of the 21st century.

Conclusion

The US Intelligence Community today is much more than technical collection agencies in league with an espionage service. It is one of the world's largest information

companies, which is directly challenged by the IT revolution to exploit the glut of open-source information; to access the best sources of expertise on national security issues, wherever they may reside; and to make the operational focus global—including for domestic intelligence. The IT revolution has literally transformed the IC workplace, significantly raised its customers' expectations in Washington and in the field, and fast-forwarded the movement of the complicated and dangerous world it covers.

Transformation affects all players in the IC, who must see intelligence more as a collaborative and less as a competitive business. Technical collectors, primarily the National Security Agency and the National Geospatial-Intelligence Agency, are challenged as never before to combine resources, to exploit together technologies of common application, and to integrate their collection strategies. And the espionage service, in its mission to "steal secrets," is impelled to blend foreign and domestic perspectives, to fuse classified and unclassified information, and to collaborate with other collection disciplines in the difficult effort to penetrate evasive, fast-moving targets.

On domestic intelligence, we are challenged to build a national collaborative network—including Federal, state, and local governments, and the private sector—that can bring together in real time the best information, the foremost experts, and well trained first responders to meet any threat to the homeland. This is the goal. Achieving it is a long-term proposition in which we must confront the twin obstacles of smarter, more capable adversaries and of persistent, change-resistant US bureaucracies. We know there will be no easy fixes. The core challenge for the Executive Branch and the Congress is to set the right direction and stick with it.

Opening Statement of Senator Charles Grassley
FBI Oversight Hearing, U.S. Senate Judiciary Committee

May 2, 2006

Mr. Chairman, thank you for holding this FBI oversight hearing today. While the FBI has made significant progress since 9/11, its transformation into an effective domestic intelligence service is far from complete. We will hear from the Government Accountability Office (GAO) today about a review of the FBI's computer modernization effort known as Trilogy. The GAO identified approximately $10 million in questionable or undocumented costs and recommended that the FBI retain an independent third-party to do a more comprehensive audit and determine whether certain contractors ought to return millions of dollars to the taxpayers.

The barriers to the transformation of the FBI go far beyond its troubled efforts to upgrade its computers. Last Thursday, after only eight months on the job, the FBI announced that the head of the FBI's newly created National Security Branch is retiring. The previous Director of Intelligence at the FBI stayed for less than two years. Consistent, long-term leadership in its senior management positions is critical to the FBI's success. The Bureau needs to find a way to recruit and retain senior managers with extensive counterterrorism and counterintelligence experience to set priorities and provide rank-and-file agents with steady, knowledgeable guidance.

That sort of leadership is essential if the FBI is going to change the negative aspects of its culture. Since 9/11, it has been clear that the FBI culture much change in order to effectively combat terrorism. The time of the old FBI has past. America can no longer tolerate an FBI that prizes loyalty above all else, hands out plum assignments based on personal relationships rather than merit, and emphasizes being "in charge" at the expense of cooperation with other government agencies.

Jurisdictional Pac-Man / Lack of Coordination

These old ways of thinking no longer serve to protect the American people. For far too long, the obsolete FBI culture has been a barrier to information sharing and coordination. The FBI gobbles up the jurisdiction, cases, and resources of other agencies like Pac-Man. Too many federal, state, and local law enforcement agencies view the FBI with disdain because it demands access to their intelligence, their informants, their evidence, and their resources while rarely returning the favor. Too many law enforcement officers no longer trust the FBI to deal fairly with them. One particularly disturbing example of this is the sabotaging by the FBI of a terrorism financing case that was developed in 2003 by agents of the Houston office of U.S. Immigration and Customs Enforcement (ICE). This March, former ICE Special Agent in Charge Joe Webber testified to a House Committee that the FBI hindered the processing of a wiretap request in a

terrorism financing case, causing the government to miss an opportunity to capture communications between the target of a criminal investigation and a Specially Designated Global Terrorist. Webber said he was told by friends within the FBI that if the case had been developed by the FBI instead of ICE, the wiretap would have sailed through the process. It is past time for this type of turf warfare to end. The Inspector General has just issued a report on this case, but it remains classified "secret." I have concerns that the classification decisions may have been influenced more by a desire to protect the FBI from public scrutiny than by legitimate concerns about national security.

Double Standards in Internal Discipline

The FBI culture contributes to internal problems as well, such as double standards in the FBI disciplinary process. Any perception that internal discipline is unfair can be devastating to the morale and effectiveness of FBI field agents. For far too long, rank and file agents have believed that management looks out for management. One example of preferential treatment can be found in the case of Cecilia Woods, who reported that her supervisor had engaged in illicit sexual activities with a paid informant. Rather than being rewarded for being concerned about the integrity of the Bureau, Woods says she was subjected to two investigations resulting in suspensions and a retaliatory transfer.

More recently we have learned of the case of Jennifer Smith-Love. Smith-Love was the Acting Special Agent in Charge of the FBI office in Baltimore, Maryland, during an investigation into the death of former Assistant U.S. Attorney Jonathan Luna. Smith-Love and two agents acting under her direction were the subject of allegations that they conducted an unauthorized search of another agent's laptop computer. Smith-Love's conduct during the investigation became the subject of an investigation by the FBI's Internal Investigations Section (IIS) of the FBI's Inspection Division and a review by the Inspector General's Office. The I.G. was critical of the FBI for classifying Love's conduct as a performance issue rather than as a matter of misconduct. Even though other agents contradicted Love's statements to IIS investigators, she received a promotion to a counterterrorism position in headquarters while the issues were pending. On first blush, this appears to be another case where a senior manager may have received lenient treatment. However, we need to learn more about what happened and why.

Inequities in the FBI disciplinary process destroy confidence in FBI leadership and should be unacceptable the Director, the Inspector General, and the Justice Department.

Support for Former FBI Agent Charged with Murder

In March, a New York grand jury indicted retired FBI agent Lin DeVecchio on four counts of murder. DeVecchio allegedly accepted bribes from a mob boss and supplied him with inside information that led to the deaths of at least four

people. This case sounds disturbingly familiar. The allegations are similar to those that surfaced a few years ago out of the Boston office, which led to two retired FBI agents being charged with crimes involving collusion with their high-level mafia informants.

Current and former FBI officials have been publicly raising money for DeVecchio's legal defense and more than forty agents appeared at his bond hearing to show support. According to the website maintained by DeVecchio's supporters in the FBI, the agents helped post a one million dollar bond to secure his release, and after the hearing, the agents surrounded DeVecchio "in a human blanket" as he left the courtroom so that he could not be questioned by reporters. One agent wrote, "it might even be said that a few reporters received a few body checks out on the sidewalk" and that he "was never prouder to be an FBI Agent."

Obviously, Mr. DeVecchio is innocent until proven guilty, and an indictment is just an allegation until proved in court. However, I am concerned about the public perception created by such aggressive and broad support of DeVecchio by current and former FBI personnel. It could leave the impression that the FBI as an institution is circling the wagons to defend itself as well as DeVecchio against the charges. I am interested in hearing Director Mueller's reaction to these events.

The Moussaoui Case and Charges of Careerism

Protecting careers has to take a back seat to protecting the American people. Unfortunately, we have seen examples where those priorities aren't in order. A few weeks ago, Minneapolis FBI agent Harry Samit testified during the sentencing hearing for Zacharias Moussaoui. What he said was startling. Agent Samit said that he warned his FBI supervisors more than 70 times before 9/11 that Moussaoui was a terrorist. He said that Supervisory Special Agent Michael Maltbie had failed to support his efforts to obtain warrants to search Moussaoui's apartment and laptop computer. Maltbie reportedly removed from a search warrant application crucial information indicating that Moussaoui had been a recruiter for a Muslim group in Chechnya linked to Osama Bin Laden. In his sworn testimony Agent Samit described the failures of FBI management as "obstructionism, careerism, and criminal negligence." As a result, Agent Samit was unable to obtain the warrants he sought. Moussaoui's computer and apartment were not searched until after 9/11. We can only guess whether 3,000 victims could have been spared by a more aggressive investigation of Moussaoui pre-9/11. However, it is certain that those who blocked the Moussaoui investigation have been rewarded rather than held accountable. The supervisor who failed to support Agent Samit's Moussaoui investigation is now in charge of the Joint Terrorism Task Force in one of our nation's largest cities.

Whistleblower Protections

The FBI's emphasis on loyalty is devastating to whistleblower protections. I continue to be concerned about whether the FBI makes any real attempt to prevent retaliation against whistleblowers. Director Mueller has often said that he will not tolerate retaliation, but actions speak louder than words.

Earlier this year, the Inspector General found that FBI Undercover Operations Unit Chief Jorge Martinez retaliated against Special Agent Michael German for raising concerns about unauthorized surveillance in a Florida terrorism investigation. After German wrote a letter outlining his concerns, Martinez said that he would never again work another undercover case and would never again be selected as an instructor at the FBI's undercover schools. Now that the IG has confirmed this key aspect of German's allegations, the question becomes whether the FBI is capable of holding its own accountable.

Another example is Bassem Youssef, the FBI's highest ranking Arab-American agent. Youssef is a native Arabic speaker and has extensive counterterrorism experience. He raised concerns after 9/11 that the FBI wasn't taking advantage of his expertise. After he made no progress internally, Youssef contacted his congressman who then contacted the Director. Youssef has now learned that he was about to receive a transfer to the International Terrorism Operations Section (ITOS) where he could have a more valuable asset to the FBI. But, after he contacted Congress, his transfer was never completed. That creates an appearance of retaliation. Chairman Specter, Senator Leahy, and I have jointly asked that these circumstances be investigated.

Trilogy / Sentinel

On our second panel today, we will hear from GAO, which found in its recent report that the FBI may have overpaid one contractor, on its Trilogy computer modernization project by $2.1 million. The report describes how another contractor on the project could not support almost $3 million that it paid to an event planning company. GAO recommended that GSA and the FBI (1) further investigate whether contractors were was overpaid, (2) determine whether other questionable costs in the report, which total more than $10 million, should be reimbursed, and (3) engage an independent third party to conduct further follow-up audit work.

The FBI has had the draft of this GAO report for months, so it knew about the millions in questionable payments Trilogy contractors identified in the report. Now two of these contractors are part of the Lockheed Martin team that was just awarded the contract the FBI's case management system, Sentinel. What assurances do the taxpayers have that the FBI will be able to recover any funds these companies owe to the government before we start paying them millions more for work on Sentinel? GAO's recommendation that there be further audit work on the Trilogy project should be taken seriously, as there may be even more taxpayer money to recover.

Conclusion

The FBI's culture limits its potential for success by putting too much emphasis on protecting its own jurisdictional turf, protecting management from allegations of misconduct, and protecting individual careers. Instead, the FBI should be focusing more on protecting the American people. We've been calling for changes in the FBI for long enough. I hope that we are going to start seeing some results.

from the office of

Senator Edward M. Kennedy

of Massachusetts

FOR IMMEDIATE RELEASE
May 2, 2006

CONTACT: Laura Capps/Melissa Wagoner
(202) 224-2633

OPENING STATEMENT BY SENATOR EDWARD M. KENNEDY AT FBI OVERSIGHT HEARING
(AS PREPARED FOR DELIVERY)

No challenge we face is more important than dealing effectively with the terrorist threat facing the nation, and reform of the FBI is an essential part of meeting that challenge.

We all agree on the need for strong powers for law enforcement and intelligence officers to investigate terrorism, prevent future attacks, and improve information-sharing between federal, state and local law enforcement. In the wake of the tragic events on September 11th, Congress, the Administration and the country face the urgent need to do everything possible to strengthen our national security and our counterterrorism efforts.

On 9/11, we were united in our commitment to protect our country, to respond aggressively to terrorism, and to destroy Al Qaeda. This was not an issue of party or, partisan politics. We all worked together.

Unfortunately, however, we are now at an impasse where the Administration refuses to work with Congress and it is putting our national security and the public's trust at risk. There is a way to fight terrorism within the framework of our Constitution. As Supreme Court Justice Robert Jackson wrote in 1941, the Constitution is not a suicide pact.

Thirty years ago, when the Cold War threatened our security, a Republican administration and a Democratic Congress worked together to pass the Foreign Intelligence Surveillance Act, giving broad authority to the government in cases involving our national security.

Then, as now, the debate was driven by reports of "watch lists" and sweeping surveillance programs. Then, as now, the American people had questions about the proper scope of the President's authority.

Today, the "politics of fear" seems to be driving our national security policy. At the same time, there are fundamental questions about whether we are getting it right. There are new concerns that we may not be any safer now than we were four years ago. I hope you can address some of the concerns about the job the FBI is doing to get its house in order and meet the terrorist threat.

###

Statement of Senator Patrick Leahy,
Ranking Member, Committee on The Judiciary
Hearing on FBI Oversight
May 2, 2006

Mr. Chairman, thank you for convening today's FBI oversight hearing. This is another opportunity to continue our efforts to remake the FBI into a modern domestic intelligence and law enforcement agency.

As you know, oversight of the FBI to help make the Bureau as good as the American people need it to be was one of my highest priorities when I chaired the Committee in the period just before and then in the wake of the attacks of 9/11. After the attacks, Congress acted quickly to address the new challenges facing the Bureau, by giving it new tools to combat terrorism, by funding information technology, and by pushing to correct institutional and management flaws that prevented FBI field agents from operating at their full potential. As recognized by Inspector General Fine, the Government Accountability Office, and others, the FBI has improved. Yet we continue to see some of the same problems that this Committee identified years ago in those earlier hearings, and that we and the 9/11 Commission sought to correct. Today, four-and-a-half years after 9/11, it troubles me deeply that the FBI is still not as strong and as equipped as it must be to fulfill its core missions.

Director Mueller, you, your leadership team and the hard-working men and women of the FBI deserve – and have – the constant appreciation of all of us as Americans, for all that you do and for the sacrifices that you make. For decades – and especially since 9/11 – the men and women of the FBI have toiled tirelessly, while under great pressure, to carry out the Bureau's duties. Constructive oversight of the FBI's work by Congress is an invaluable tool to help keep moving us toward the goals that we all share for the Bureau. That is why you and we are here today.

Domestic Surveillance

Since 9/11, the Bureau has made great strides in enhancing its intelligence gathering capabilities. I was disappointed to learn, however, that the FBI has been using that capability to conduct domestic surveillance on law-abiding American citizens, simply because they happen to oppose the government's war policy in Iraq. In March, the *Seattle Post-Intelligencer* reported that federal antiterrorism agencies, including the FBI, conducted surveillance on longtime Quaker peace activist Glen Milner during the 2003 Seafair festival. A Freedom of Information Act lawsuit recently filed by the ACLU has also revealed communications between the FBI and other law enforcement agencies about the surveillance of several other domestic peace groups. The FBI cannot simply dismiss these very serious concerns by citing Inspector General Fine's recent report on

the Bureau's conduct during the 2004 nation political conventions. That report does not address these other incidents of domestic surveillance.

According to the documents obtained in that lawsuit, these are not isolated events. The documents show that the FBI has infiltrated political, environmental, antiwar and faith-based groups elsewhere across the country.

The FBI's participation in domestic spying - at the expense of the privacy and civil liberties interests of our citizens - is also evident in a recent report on the Bureau's surveillance activities. According to a recent report by Inspector General Fine, the FBI reported more than 100 possible surveillance violations to the Intelligence Oversight Board during the past two years. These violations included cases in which FBI agents tapped the wrong telephone, intercepted the wrong emails or continued to listen to conversations more than a year after a warrant had expired.

Now we learn that the FBI wants to search the personal records of prominent Washington reporter Jack Anderson, just a few months after his death, to look for documents that may have been classified at some distant point in time.

All of this should concern all who value privacy rights and the free exchange of ideas in our society.

Information-Sharing, Terrorist Screening Center, And Terrorist Watchlist

I have closely followed the FBI's challenges in analyzing and disseminating the intelligence data in its possession. The failure of our intelligence and law enforcement agencies to share information that might have warned of a pending terrorist attack was cited as a key problem in the investigations that followed the 9/11 attacks. Last month, the GAO issued a report finding that, despite more than four years of legislation, Executive Orders and presidential directives, the Bush Administration has yet to comprehensively improve the sharing of counterterrorism information among dozens of federal agencies -- including the FBI. In fact, numerous deadlines set by both President Bush and by Congress to better coordinate information sharing have not been met.

According to the GAO's report, the FBI does have several initiatives underway to promote information sharing, including the establishment of 103 joint terrorism task forces around the country. While commendable, this effort is not fully effective because, as the GAO found, there are no government-wide standards on how to handle the sensitive counterterrorism information that the FBI must share with its law enforcement partners.

The Terrorist Watchlist produced and disseminated by the FBI's Terrorist Screening Center has been plagued by too many entries and inaccurate and incomplete information. Earlier this year, the *Washington Post* reported that the National

Counterterrorism Center - which provides data for the watchlist - maintains a central repository of 325,000 names of international terrorist suspects. The Terrorist Screening Center provides these names to the Transportation Security Agency for its no-fly list, the State Department for its visa program, the Department of Homeland Security for border crossings, and the National Crime Information Center for distribution to police.

If being placed on a list means in practice that you will be denied a visa, barred entry, put on the no-fly list, or targeted for prosecution, then the sweep of this list and the apparent absence of any way to clear oneself certainly raises privacy concerns as well as law enforcement problems. The FBI must take steps to better ensure the accuracy of the watchlist and to protect the privacy of the growing number of law-abiding Americans who names have been improperly listed there.

Virtual Case File And Sentinel

It is no secret that I - like many Americans - am greatly concerned about the FBI's handling of the now defunct Trilogy project and the prospects for its replacement - the Sentinel project. The sad saga of the Trilogy project is well known to everyone in this room. The project, which was intended to modernize the FBI's information technology infrastructure, was plagued by numerous schedule delays and cost increases - from an estimated $380 million to an estimated $458 million to upward of $596 million, before it was finally scrapped last year.

In March, the GAO issued its report to Congress on the Trilogy case management project. That report found that weak controls on the parts of the FBI and the General Service Administration resulted in the Bureau paying more that $10.1 million in unallowable costs and in the FBI being unable to account for more than 1,400 pieces of missing equipment, valued at about $8.6 million. The GAO also cautioned in its report that if these control weaknesses go uncorrected, future contracts - including those related to Sentinel - will be highly exposed to improper payments and similar problems.

As the Director knows from the recent Appropriations subcommittee hearing, I find it intolerable that Congress - and this Committee in particular -- was not given the full story on Trilogy until the entire project collapsed under its own weight. Taxpayers are out millions of dollars, and we have lost several crucial years in getting this essential task completed.

In March, we learned that Sentinel will cost the American taxpayers $425 million to complete and that this system will not be fully operational until 2009. The GAO's recommendations will be critical as we move forward with the Sentinel project and attempt to manage the already skyrocketing costs of that replacement program. I remain very concerned about this project. This time around, I expect transparency and accountability. The Bureau's effectiveness hangs in the balance, and the American people cannot afford another fiasco.

Counterintelligence And Counterterrorism

There are also other weaknesses in the Bureau's critical counterintelligence and counterterrorism efforts. I continue to be troubled by the relatively low level of counterterrorism experience of some of the FBI's mid-level and senior counterterrorism officials. Director Mueller recently told us that candidates for mid-level Special Agent positions within the FBI are vetted through a process in which subject matter expertise is considered and preferred, but is not mandatory. In other words, counterterrorism experience is not a prerequisite to promotion to managerial positions within the Bureau. Given that the FBI's top priority since 9/11 is to protect the United States from terrorist attacks, I believe that is critical that we have managers within the FBI who have significant counterterrorism experience. The FBI simply cannot continue to foster a culture that places a lower value on intelligence functions than investigative efforts.

Conclusion

Since 9/11, the FBI has made significant strides to adjust to the threats and challenges of our time. I commend Director Mueller and the Bureau for all that they have accomplished, but there is much more work to do. I look forward to engaging our witnesses on how best to move forward.

#####

STATEMENT OF
ROBERT S. MUELLER, III
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
BEFORE THE
UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
May 2, 2006

Good morning, Mr. Chairman, Senator Leahy, and Members of the Committee. I am pleased to appear before you today to update you on the current state of the FBI, as well as our plans for the near future. I would also like to thank the Committee for your continued oversight of the Bureau and your efforts to ensure our success as we pursue the shared goal of making America safer, while preserving our civil liberties.

As this Committee knows, much of the last year has been devoted to a national discussion about the tools that should be afforded to the men and women engaged in the fight against terrorism, both at home and abroad. I want to thank the Committee for your work in producing a balanced law reauthorizing the USA PATRIOT Act. Through your efforts, our Agents will retain the tools necessary to wage an effective fight against terrorism, within a framework that ensures important safeguards for civil liberties and enhanced judicial and congressional oversight.

For the FBI, the primary tools used in our efforts to detect, disrupt and prevent acts of terrorism continue to be those included in, or enhanced by, the USA PATRIOT Act and related laws, including: the court authorized surveillance of international terrorists; the sharing of key intelligence information; and the collection of relevant documents pursuant to court orders or through National Security Letters. Of course, as I have explained to this Committee before, we still believe that administrative subpoenas -- such as those available in narcotics and health care fraud cases -- would be appropriate in the counterterrorism arena. Accordingly, it is my hope that the forthcoming review of the FBI's use of National Security Letters -- which is being conducted by the Department of Justice (DOJ) Office of Inspector General (OIG) pursuant to the reauthorized PATRIOT Act -- will underscore the FBI's responsible use of such authorities.

As this Committee may recall, shortly after the Republican and Democratic National Conventions in the Summer of 2004, media reports stated that the FBI had questioned political demonstrators across the country in advance of the conventions, leading civil liberties groups to allege that the FBI was attempting to chill protestors from exercising their First Amendment rights. At the request of Congress, the DOJ-OIG conducted an investigation and, last week, released its final report on this matter. The OIG did <u>not</u> substantiate the allegations and concluded that all interviews conducted by the FBI of potential convention protestors were conducted "for legitimate law enforcement purposes" and were conducted consistent with the Attorney General Guidelines. I am pleased, but not surprised, by the OIG's findings. The men and women of the FBI understand and appreciate the power entrusted to them and are vigilant in their efforts to protect the country while respecting civil liberties.

I would like to take the opportunity this morning to update you on three areas of ongoing interest to the Committee: our progress in establishing a vigorous intelligence service within the FBI; developments in our efforts to modernize the FBI's Information Technology program, especially the recent award of a contract to Lockheed Martin in connection with the Sentinel program; and the latest results of our efforts to reshape the FBI's human resources function.

NATIONAL SECURITY BRANCH

I last appeared before the Committee just one month after the President approved the recommendations of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, commonly known as the WMD Commission. These included a recommendation regarding the establishment of an intelligence service within the FBI. I am pleased to report that FBI's National Security Branch (the "NSB") has been established to ensure the integration of the FBI's primary national security programs under the leadership of a single Executive Assistant Director, and to implement policies and initiatives designed to enhance the capability of the entire FBI to support its national security mission.

Although still relatively new, the NSB is making significant progress in integrating the missions, capabilities, and resources of the Counterterrorism, Counterintelligence, and Directorate of Intelligence programs. The FBI is currently working with the Department of Justice and the Administration to ensure that the NSB meets the directives set forth by the President and is responsive to the Office of the Director of National Intelligence (ODNI).

While I am optimistic about the new NSB, I am aware that some harbor doubts about the FBI's ability to transform itself into a leading intelligence agency. Such critics often cite the mistaken belief that the intelligence mission and the law enforcement mission are inherently incompatible. They also contend that the FBI is reluctant to share information with its partner agencies.

I believe it is important to note that both 9/11 Commission and the WMD Commission found that the intelligence and law enforcement functions should not be separated. They understood that intelligence developed in criminal investigations could be relevant to ongoing intelligence matters. In addition, many of the skills necessary to a successful criminal investigation are mirrored in the intelligence arena. The need to cultivate confidential informants and build rapport with cooperating witnesses, the ability to follow complex money trails, the ability to decipher the coded language of gang members or drug dealers, and the know-how to extract meaning from a collection of seemingly unrelated clues are all skills that can be -- and are -- applied to intelligence matters.

With regard to information sharing, we have doubled the number of intelligence analysts, and in every field office we have established Field Intelligence Groups, or FIGs -- agents and analysts working together with one shared mission -- to leverage intelligence to protect our nation. From January 2004 through January 2006, Intelligence Analyst staffing increased on the

FIGs by 61 percent, from 617 to 995. This increase in analysts has helped to fuel our sharing of intelligence products. Since September 11th, we have disseminated more than 20,000 intelligence reports, assessments, and bulletins to our partners.

While our national security efforts remain our top priority, we continue to fulfill our crime-fighting responsibilities as well. Public corruption is the top criminal priority for the FBI. Over the last two years, our investigations have led to the conviction of over 1,000 government employees involved in corrupt activities, to include 177 federal officials, 158 state officials, 360 local officials, and more than 365 police officers.

We also continue to focus on implementing the National Gang Strategy, along with ATF. This strategy is designed to identify the prolific and violent gangs in the United States and to aggressively investigate, disrupt, and dismantle their criminal enterprises through prosecution under appropriate laws.

INFORMATION TECHNOLOGY

When it comes to analyzing information, technology is crucial. As this Committee knows, on March 16, 2006, we announced the award of the contract for development of the Sentinel program to Lockheed Martin. Under the terms of the $305 million contract, Lockheed Martin and its industry partners will use proven commercial off-the-shelf technologies to produce an integrated system that supports processing, storage and management of the FBI's current paper-based records system. The program includes an incremental development and delivery of Sentinel capabilities, including $73 million for operations and maintenance activities.

Now that the contract has been awarded, we are moving forward with phase one of the development process. Each of the four phases will introduce new stand-alone capabilities and will be user-focused. As each phase is implemented, existing information will be transferred to new systems and old legacy systems will be retired.

I want to emphasize that the Sentinel program is not a reincarnation of the Virtual Case File. Not only will Sentinel provide greater capabilities, it will be deployed on an incremental basis over four years. And, to prevent any missteps, each phase of the Sentinel contracting process is being closely scrutinized by a team of FBI technical experts, the Government Accountability Office, the Office of Management and Budget, and the Department of Justice's Chief Information Office and Inspector General. Furthermore, at the urging of Congress, we have also engaged outside experts to help us review and assess the implementation of Sentinel.

Significantly, the FBI also has established contractual mechanisms to monitor contractor performance, and has structured the program so that all, or portions, of the effort can be terminated upon identification of poor performance, including:

- A scheduled control and monitoring system that will identify variances in the contractor's schedule every two weeks.

- Imposition of the requirement on both the prime contractor and the Sentinel Program Management Office to use a certified Earned Value Management ("EVM") System, as well as the requirement to report on EVM status on a monthly basis. Certification of these EVM Systems includes Independent Validation and Verification by an independent entity.

- And, establishment of an award fee structure tied to contract performance measurements.

I have met with the CEO of Lockheed Martin and we are committed to working together to ensure successful deployment of each phase of Sentinel. We will also continue to update this Committee on the progress of Sentinel and will ensure that the Committee staff receives briefings throughout the development process.

Without minimizing the challenges we have had in the past, I think it is also important to underscore the improvements that have already been achieved in our efforts to modernize the FBI's Information Technology.

Today, when an FBI agent sits down at her desk and logs on to the computer, she is connected at the "secret" level to a fast, secure system that allows her to send e-mails, photographs and documents to any other agent or analyst in the Bureau -- across the country and around the world. Agents also have direct access to the FBI's internal "Intranet," which can be searched via a Google-based search engine. Through this Intranet, agents can receive online training, watch streaming video of meetings or conferences, download investigative guidelines, or even review the latest congressional testimony of FBI Executives.

For "top secret" communications, we have deployed the Top Secret/Sensitive Compartmented Information Operational Network, or SCION. Nearly 4,000 personnel have been trained on the SCION and associated Intelligence Community systems. This system is the backbone for FBI personnel to coordinate, collaborate, disseminate and conduct research on analysis with the Intelligence Community.

Additionally, other technology initiatives, such as the Investigative Data Warehouse ("IDW"), have surpassed our expectations. As this Committee knows, the IDW is a centralized repository for relevant counterterrorism and investigative data that allows users to query the information using advanced software tools. IDW now contains over 560 million FBI and other agency documents from previously stove-piped systems. Nearly 12,000 users can access it via the FBI's classified network from any FBI terminal throughout the globe. And, nearly thirty percent of the user accounts are provided to task force members from other local, state and federal agencies.

Finally, we have established an interface whereby FBI Field Offices can access the data mart of the Foreign Terrorist Tracking Task Force, or FTTTF. This access allows FTTTF analysts to use both government and commercial data to assist those evaluating whether a foreign

individual suspected of terrorist activity or support should be denied entry into the United States or, if already in this country, to help them locate, detain, prosecute, or deport these individuals, as appropriate.

We have worked hard to build a solid foundation for the successful implementation of major Information Technology investments and these are just a few examples of proven success. We have instituted strong, centralized management of IT assets, including strategic planning, portfolio management, and enterprise architecture, and we require compliance with disciplined policies, procedures, and business practices that govern the management of IT projects from "cradle to grave."

HUMAN RESOURCES

While technology is critical to our mission, the men and women of the FBI remain our most important asset. Their talent, creativity, and commitment to the public good are the true keys to our success. Accordingly, we continue to reshape our human resources program to recruit, hire, train, and retain quality individuals for our expanding human capital needs.

When I last testified before the Committee, I informed you that we had hired an executive search firm to identify a Chief Human Resources Officer for the FBI with significant experience in transformation of human resources in a large organization. At the conclusion of this search, on October 11, 2005, we appointed Don Packham as the FBI's Chief Human Resources Officer. Mr. Packham has served in a number of senior human resources roles, most recently with the British Petroleum Corporation. In his last position with BP, Mr. Packham was the Senior Vice President of Human Resources for the Americas, where he oversaw human resources for 50,000 employees spread across more than 50 business units in North and South America.

I am confident that Don Packham is the right person to help us continue the transformation of our workforce. Many changes are already underway. Last year, Congress provided the FBI with the legislative authority and resources to help us compete with other homeland security and Intelligence Community organizations which often recruited employees away from the FBI. The funding allowed us to provide recruitment bonuses for potential new hires, retention and relocation bonuses to existing employees with job offers from other government entities, and increased funding for our University Education Program and student loan repayments.

Of course, human resources programs do not exist in a vacuum. They must be integrated with our larger mission. For this reason, we have sought to include entities like the NSB in the process of improving our human resources. The human resources initiatives the NSB is undertaking include defining core national security competencies and revising recruiting practices to target applicants with those competencies, and implementing a four-stage national security career path that will result in career-long specialization for Intelligence Analysts and Special Agents.

Finally, I know that one area of concern for this Committee has been the rate of turnover among the FBI's leadership ranks. As recognized by the National Academy of Public Administration, we have launched a number of initiatives to address this issue. Representatives of the FBI's Executive Development and Selection Program are working with the RAND Corporation to develop a database designed to assist in Senior Executive Service (SES) succession planning. In addition, the FBI's Training and Development Division is formulating an "FBI Leadership Training Framework" that will provide the basis for a comprehensive leadership development program.

Another piece of the FBI's leadership development strategy is the Strategic Leadership Development Plan, which will provide techniques for identifying leadership needs and problems, articulate a program designed to enhance leadership knowledge, skills, and abilities throughout an employee's career, and relate leadership development to the FBI's strategic mission in its top priority programs. The FBI is evaluating several possible measures to lengthen tenure in SES positions, particularly at FBI Headquarters, including the increased use of retention bonuses and other incentives to encourage SES employees to remain in these positions longer. With strong, steady leadership, we will be better poised to achieve our mission of protecting America.

CONCLUSION

Mr. Chairman, Senator Leahy, and Members of the Committee, today's FBI is part of a vast national and international campaign dedicated to defeating terrorism. Working hand-in-hand with our partners in law enforcement, intelligence, the military and diplomatic circles, the FBI's primary responsibility is to neutralize terrorist cells and operatives here in the United States and help dismantle terrorist networks worldwide. Although protecting the United States from terrorist attacks is our first priority, we remain committed to the defense of America against foreign intelligence threats as well as the enforcement of federal criminal laws, all while respecting and defending the Constitution.

This year will mark the five-year anniversary of September 11th. The FBI has changed dramatically since the terrorist attacks and we will continue to evolve to meet the emerging threats to our country. We have expanded our mission, radically overhauled our intelligence programs and capabilities, and have undergone tremendous personnel growth. I thank you for your consistent support of the FBI as we continue this transformation, and I am happy to answer any questions you may have.

Copyright 2006 The New York Times Company
The New York Times
April 19, 2006 Wednesday
Late Edition - Final

SECTION: Section A; Column 1; National Desk; Pg. 1
LENGTH: 862 words
HEADLINE: F.B.I. Is Seeking To Search Papers Of Dead Reporter
BYLINE: By SCOTT SHANE
DATELINE: WASHINGTON, April 18

BODY:
The F.B.I. is seeking to go through the files of the late newspaper columnist Jack Anderson to remove classified material he may have accumulated in four decades of muckraking Washington journalism.

Mr. Anderson's family has refused to allow a search of 188 boxes, the files of a well-known reporter who had long feuded with the Federal Bureau of Investigation and had exposed plans by the Central Intelligence Agency to kill Fidel Castro, the machinations of the Iran-contra affair and the misdemeanors of generations of congressmen.

Mr. Anderson's son Kevin said that to allow government agents to rifle through the papers would betray his father's principles and intimidate other journalists, and that family members were willing to go to jail to protect the collection.

"It's my father's legacy," said Kevin N. Anderson, a Salt Lake City lawyer and one of the columnist's nine children. "The government has always and continues to this day to abuse the secrecy stamp. My father's view was that the public is the employer of these government employees and has the right to know what they're up to."

The F.B.I. says the dispute over the papers, which await cataloging at George Washington University here, is a simple matter of law.

"It's been determined that among the papers there are a number of classified U.S. government documents," said Bill Carter, an F.B.I. spokesman. "Under the law, no private person may possess classified documents that were illegally provided to them. These documents remain the property of the government."

The standoff, which appears to have begun with an F.B.I. effort to find evidence for the criminal case against two pro-Israel lobbyists, has quickly hardened into a new test of the Bush administration's protection of government secrets and journalists' ability to report on them.

F.B.I. agents are investigating several leaks of classified information, including details of domestic eavesdropping by the National Security Agency and the secret overseas jails for terror suspects run by the C.I.A.

In addition, the two lobbyists, former employees of the American Israel Public Affairs Committee, or Aipac, face trial next month for receiving classified information, in a case criticized by civil liberties advocates as criminalizing the routine exchange of inside information.

The National Archives recently suspended a program in which intelligence agencies had pulled thousands of historical documents from public access on the ground that they should still be classified.

But the F.B.I.'s quest for secret material leaked years ago to a now-dead journalist, first reported Tuesday in the Chronicle of Higher Education, seems unprecedented, said several people with long experience in First Amendment law.

"I'm not aware of any previous government attempt to retrieve such material," said Lucy Dalglish, executive director of the Reporters Committee for Freedom of the Press. "Librarians and historians are having a fit, and I can't imagine a bigger chill to journalists."

The George Washington University librarian, Jack Siggins, said the university strongly objected to the F.B.I.'s removing anything from the Anderson archive.

"We certainly don't want anyone going through this material, let alone the F.B.I., if they're going to pull documents out," Mr. Siggins said. "We think Jack Anderson represents something important in American culture -- answers to the question, How does our government work?"

Mr. Anderson was hired as a reporter in 1947 by Drew Pearson, who bequeathed to him a popular column called Washington Merry-Go-Round.

Mr. Anderson developed Parkinson's disease and did little reporting for the column in the 15 years before his death in December at 83, said Mark Feldstein, director of the journalism program at George Washington, who is writing a book about him.

His files were stored for years at Brigham Young University before being transferred to George Washington at Mr. Anderson's request last year, but the F.B.I. apparently made no effort to search them.

Kevin Anderson said said F.B.I. agents first approached his mother, Olivia, early this year.

"They talked about the Aipac case and that they thought Dad had some classified documents and they wanted to take fingerprints from them" to identify possible sources, he recalled. "But they said they wanted to look at all 200 boxes and if they found anything classified they'd be duty-bound to take them."

Both Kevin Anderson and Mr. Feldstein, the journalism professor, said they did not think the columnist ever wrote about Aipac.

Mr. Anderson said he thought the Aipac case was a pretext for a broader search, a conclusion shared by others, including Thomas S. Blanton, who oversees the National Security Archive, a collection of historic documents at George Washington.

"Recovery of leaked C.I.A. and White House documents that Jack Anderson got back in the 70's has been on the F.B.I.'s wanted list for decades," Mr. Blanton said.

Mr. Carter of the F.B.I. declined to comment on any connection to the Aipac case or to say how the bureau learned that classified documents were in the Anderson files.

The Plain Dealer

FBI sought phone, bank, Internet records on 3,501

Saturday, April 29, 2006
Mark Sherman
Associated Press

Washington - The FBI secretly sought information last year on 3,501 U.S. citizens and legal residents from their banks and credit card, telephone and Internet companies without a court's approval, the Justice Department said Friday.

It was the first time the Bush administration has publicly disclosed how often it uses the administrative subpoena known as a National Security Letter, which allows the executive branch of government to obtain records about people in terrorism and espionage investigations without a judge's approval or a grand jury subpoena.

Friday's disclosure was mandated as part of the renewal of the Patriot Act, the administration's sweeping anti-terror law.

The FBI delivered a total of 9,254 NSLs relating to 3,501 people in 2005, according to a report submitted late Friday to Democratic and Republican leaders in the House and Senate.

In some cases, the bureau demanded information about one person from several companies.

The numbers from previous years remain classified, officials said.

The number was a significant jump over past use of the warrant for business records.

A year ago, Attorney General Alberto Gonzales told Congress 35 warrants had been approved between November 2003 and April 2005.

The spike is expected to be temporary, however, because the Patriot Act renewal that President Bush signed in March made it easier for authorities to obtain subscriber information on telephone numbers captured through certain wiretaps.

© 2006 The Plain Dealer
© 2006 cleveland.com All Rights Reserved.

SEATTLE POST -INTELLIGENCER
Domestic spying on anti-war groups forces ACLU into action

Tuesday, March 21,2006
By MIKE BARBER
P-I REPORTER

Monica Zucker and three other members of Seattle's Raging Grannies, a peace group of older women who dress in outrageous hats and sing protest songs, lifted up their voices in response Tuesday to recent Seattle P-I disclosures that they were in federal anti-terrorism files.

"Oh, we're a gaggle of grannies, urging you off of your fannies," they sang at a news conference in the downtown Seattle offices of the American Civil Liberties Union of Washington.

Acting on behalf of the Raging Grannies and 10 other peace groups across the state, the ACLU of Washington is demanding to know whether and why federal government anti-terrorism units are spending time and money spying on peace organizations.

The local ACLU is using the Freedom of Information Act to seek information on any surveillance from the Defense Department, the FBI and the Seattle Joint Terrorism Task Force. The move was sparked by disclosures in the Seattle P-I last month. The newspaper documented government surveillance on a longtime Quaker peace activist Glen Milner, of Shoreline, and other anti-war activists during U.S. Navy fleet participation in the annual Seafair festival in recent years.

"The government should not spy on groups engaging in peaceful political protest. The FBI should focus its efforts on actual threats and not target people because of their political views," said Kathleen Taylor, state ACLU executive director.

To those who say domestic spying is a price they are willing to pay for security, Taylor echoed critics, in and out of government, who say too much useless information gums up anti-terrorism intelligence rather than helping it.

"You can't find a needle in the haystack by adding more hay," she said.

The ACLU filed the request on its own behalf, Seattle Raging Grannies and other nonviolent religious and political anti-war groups statewide:

The American Friends Service Committee; Peace and Justice Action League of Spokane; People for Peace, Justice, and Healing; Pierce County Truth in Recruiting; Seattle Peace Chorus; Sound Nonviolent Opponents of War; United for Peace of Pierce County; Vancouver For Peace; Western Washington Fellowship of Reconciliation; and the Yakima Valley Peace Advocates Network.

Several, including the Raging Grannies, were mentioned in federal law enforcement documents acquired by the P-I. Law enforcement wanted to monitor anti-war protest activities surrounding Seafair in 2003 and 2004.

Barry Steinhardt, who directs the ACLD's technology and liberty project, is pessimistic that the request will yield much. "Not only is the government resisting current (requests) but it is taking steps to put more limits upon them." Meanwhile, domestic information gathering is increasing.

Still, it's important to try, he said. Aside from the chilling effect on political dissent, information finding its way some or all of the glut of new a government information-gathering systems has the potential for misinterpretation, resulting in possible harassment, arrest - even being flagged for airport no-fly lists, he said.

Representatives from local peace organizations mentioned in federal law enforcement files said it raises other concerns for them.

"In a time of war, when we are told it will be endless war, for my government to be spending to investigate the Peace Chorus is stunning, an incredible waste of money," said Martha Baskin, a member of the Seattle Peace Chorus.

U.S. News & World Report

"High tech's High Stakes at the FBI"

A pricey computer upgrade may be hurting fieldwork

By Chitra Ragavan
4/17/06

Ever since he took office nearly five years ago, FBI Director Robert Mueller has struggled to replace his agency's antiquated computer systems. But for Mueller, the experience has been like living the movie *Groundhog Day*. He has found himself back at square one over and over again. Last year, the director reluctantly pulled the plug on a much-ballyhooed $170 million re-placement known as Virtual Case File (VCF). Now Mueller is staking his reputation on a new system known as Sentinel, which, by current estimates, will cost nearly $500 million and take four more years to deploy. But the Justice Department's inspector general, Glenn Fine, warned in a recent audit report that a lack of oversight could leave Sentinel with major cost overruns just like VCF's. And at the bureau, tensions are rising as many officials stew over what they view as imprudent across-the-board cost cutting to hide Sentinel's *real* price tag from Congress and spare Mueller further ignominy. "In meetings, the message has been 'Empty your pockets. Give us your loose change,'" one senior official told *U.S. News*.

The formal bureau line is that nothing is amiss. FBI spokesman John Miller says the Sentinel contract has "program management from inside and outside to prevent mismanagement." Miller says Fine's audit report is "very positive, on balance" about Sentinel. When VCF collapsed last year, Mueller announced his decision not to seek additional technology funds until fiscal year 2007. Instead, Mueller got Congress to approve a $97 million "reprogramming" last November including $29 million from the counterterrorism budget. This year, Mueller has asked his divisions to give back a portion of their budgets. Mueller decided we are going to "bite the bullet," one FBI official said. Last week, FBI sources say, managers were told to cough up $30 million to $40 million as part of the second go-around. "It's like a ransom demand," complained one FBI official. "They're saying, 'You'd better come up with the money or it's going to fail, and it will be on *your* head.'"

Savings. Mueller assured his team last year that the 2006 budget cuts would be restricted to administrative costs like conferences and that money for law enforcement operations would be protected. Officially, the FBI says that's still the case. But sources say the cuts have had a cascading effect--that some agents in the field have been told to use their cars judiciously and to curtail the use of informants and covert off-site rentals for undercover operations. Miller says the gas issue is unrelated to Sentinel and that the FBI's budgeting was done prior to the sharp increases in gas prices. He adds that headquarters has given field offices more than $3 million to counter any gas shortfalls.

In his audit report last month, Fine warned that passing the hat a second time could risk cutting the bureau's "mission critical" operations to the bone. Fine said the FBI has taken "important steps to address its past mistakes with VCF." But Fine said the "potential

weaknesses" in cost controls are a "significant project risk." Some executives believe the bureau's computer upgrades could ultimately total a billion dollars--double the projected costs. The FBI's Miller disagrees, saying vigorous oversight will prevent this from happening.

Many agents blame Chief Information Officer Zalmai Azmi for the on-going tech woes. When Azmi recently won a prestigious Presidential Rank Award, there was con-siderable unhappiness among the troops. Mueller has strongly backed Azmi, and Miller says Azmi has done a "tremendous job" on Sentinel.

For Mueller, there have been some technological successes. As part of the Trilogy project--of which VCF was the final phase--Mueller gave agents thousands of new computer terminals and had outdated systems and other infrastructure retooled. The bureau has a data warehouse that Miller says can search a billion records in counterterrorism cases. "It's not like we have just been sitting around and waiting," says Miller. But so far Mueller has failed in his quest for the holy grail: state-of-the-art software that will seamlessly connect his agents to one another and allow them to quickly share information.

Many bureau insiders doubt Sentinel will be their savior either. "There's an increase in chatter that's as great or greater than during VCF, that Sentinel is going to fail," says one official. "And everybody knows it but Mueller. "FBI spokesman Miller says the pessimism is unwarranted since the contract was just awarded. "It is like saying people believe a building will topple," says Miller, "before workers break ground."

The Washington Post
washingtonpost.com
The Washington Post
April 19, 2006 Wednesday
Final Edition

SECTION: A Section; A03
LENGTH: 842 words
HEADLINE: GAO Faults Agencies' Sharing of Terror Data
BYLINE: Karen DeYoung, Washington Post Staff Writer

BODY:
Despite more than four years of legislation, executive orders and presidential directives, the Bush administration has yet to comprehensively improve sharing of counterterrorism information among dozens of federal agencies -- and between them and thousands of nonfederal partners, government investigators have concluded.

Repeated deadlines set by both President Bush and Congress have not been met, according to a 34-page report issued late Monday by the Government Accountability Office. While acknowledging the "complexity of the task," the report notes that responsibility for the effort has shifted since late 2001 from the White House to the Office of Management and Budget to the Department of Homeland Security, and now resides with the director of national intelligence. "None has yet completed the task," the report noted.

The GAO expressed "disappointment" that Director of National Intelligence John D. Negroponte declined to address its findings beyond a letter saying that "the review of intelligence activities is beyond GAO's purview." Senate Homeland Security Committee Chairman Susan Collins (R-Maine), who requested the investigation along with several House chairmen, issued a statement yesterday regretting the DNI response and noting that she co-sponsored the 2004 law that mandated the information-sharing and created Negroponte's job.

The failure of intelligence and law enforcement agencies to share information that might have warned of a pending terrorist attack was cited by investigations that followed the Sept. 11, 2001, attacks. Delays in developing a comprehensive system to link counterterrorism efforts and information among federal agencies have long been attributed to what Negroponte has called their individual "cultures" and a reluctance to cooperate with one another.

Last spring, the president appointed a "program manager" in Negroponte's office to develop what is formally known as an "Information Sharing Environment," or ISE, across the entire government. In October, Bush issued an executive order setting priorities for developing a system, followed on Dec. 19 by a presidential memorandum requiring all executive department and agency heads to support ISE efforts.

In January, ISE manager John Russack, an intelligence veteran, resigned after complaining of inadequate staffing and budget. A new manager, former State Department counterterrorism adviser Thomas E. McNamara, was named by the

White House last month. A new deadline for the ISE system has been set for December.

The GAO report cited several initiatives underway. They include the establishment by the **FBI** of 103 joint terrorism task forces around the country staffed with **FBI** officers as well as state and local law enforcement officers; **FBI**-Department of Homeland Security collaboration in distributing terrorism-related intelligence bulletins to local law enforcement, and the creation of the National Counterterrorism Center (NCTC).

The NCTC was established to prevent individual agencies from hoarding terrorism information. It collects and analyzes terrorist threat information from 26 different government databases and shares it online with what NCTC spokesman Mark Mansfield said are "about 5,500 users from throughout the federal counterterrorism community, a more than 30 percent increase in the past year alone."

The report did not fault the NCTC operation but noted the lack of "government-wide policies and processes to help agencies integrate the myriad of ongoing efforts to improve the sharing of terrorism-related information that is critical to protecting our homeland."

It was particularly critical of the lack of standards for "sensitive but unclassified homeland security information" that is subject to limited distribution and not to be made public. A wide range of federal agencies including the departments of Defense, Justice, Treasury and Homeland Security reported using 56 different designations to identify such information, including "For Official Use Only," "Protected Critical Infrastructure Information," "Limited Distribution Information" and "Sensitive Information."

Many use the same terms, but with widely different definitions, or use different terminology or restrictive phrases for what is essentially the same information. Most of the 26 federal agencies surveyed reported they had no firm policies for such designations or individuals specifically authorized to impose them.

In a reflection of ongoing mistrust, 11 of the agencies said they had concerns about the ability of other parties to protect sensitive information, and some complained that information disseminated to state and local partners had on occasion been posted on public Web sites.

State and local first responders told GAO investigators that the multiplicity of designations and lack of common federal standards "not only causes confusion but leads to an alternating feast or famine of information" that either left them in the dark or overwhelmed them with identical information from multiple federal sources.