AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 108–555

DEPARTMENT OF HOMELAND SECURITY'S BUDGET SUBMISSION FOR FISCAL YEAR 2005

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

FEBRUARY 9, 2004

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

92–688 PDF WASHINGTON : 2005

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 GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
ARLEN SPECTER, Pennsylvania
ROBERT F. BENNETT, Utah
PETER G. FITZGERALD, Illinois
JOHN E. SUNUNU, New Hampshire
RICHARD C. SHELBY, Alabama

JOSEPH I. LIEBERMAN, Connecticut
CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
RICHARD J. DURBIN, Illinois
THOMAS R. CARPER, Delaware
MARK DAYTON, Minnesota
FRANK LAUTENBERG, New Jersey
MARK PRYOR, Arkansas

MICHAEL D. BOPP, *Staff Director and Chief Counsel*
TIM RADUCHA-GRACE, *Professional Staff Member*
JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Counsel*
HOLLY A. IDELSON, *Minority Counsel*
AMY B. NEWHOUSE, *Chief Clerk*

CONTENTS

Opening statements:	Page
Senator Collins	1
Senator Lieberman	3
Senator Levin	5
Senator Akaka	15
Senator Durbin	18
Senator Pryor	19
Senator Sununu	28

WITNESS

MONDAY, FEBRUARY 9, 2004

Hon. Tom Ridge, Secretary, U.S. Department of Homeland Security:	
Testimony	20
Prepared Statement	47

APPENDIX

Questions and Responses submitted for the Record for Secretary Ridge from:	
Senator Sununu	55
Senator Collins	56
Senator Carper	60
Senator Fitzgerald	66
Senator Bennett	78
Senator Akaka	95
Senator Lautenberg	106
Senator Lieberman	108
Senator Specter	146

DEPARTMENT OF HOMELAND SECURITY'S BUDGET SUBMISSION FOR FISCAL YEAR 2005

MONDAY, FEBRUARY 9, 2004

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:02 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Lieberman, Levin, Akaka, Durbin, Pryor, and Sununu.

OPENING STATEMENT OF SENATOR COLLINS

Chairman COLLINS. The Committee will come to order.

Good morning. I want to begin by welcoming Secretary Ridge here this morning and thank him for making his third appearance before the Committee on Governmental Affairs.

I also want to welcome back to the Committee our friend and colleague, the Committee's Ranking Democrat, Senator Joseph Lieberman. Joe, we have missed you greatly in the last few months and we are very glad to have you back. I personally believe that your philosophy resonates with a broad range of politically moderate Americans (which would of made you a formidable force in the general election). For that reason, I am really glad to have you back. It is a great pleasure to again have you back at my side.

Senator LIEBERMAN. Thank you very much.

Chairman COLLINS. It has been nearly 2½ years since an unconscionable act of war was committed against the United States. The American people responded to the attacks of September 11 with courage, courage that was evident that horrible day in the heroic actions of the passengers on Flight 93, in the firefighters and police officers at Ground Zero, and in the Pentagon employees who led their co-workers to safety through fire, smoke, and rubble.

That courage is also evident today in the men and women of our Armed Forces who are serving on the front lines in the war on terrorism and in the ordinary Americans across the country who carry on normal, productive lives, refusing to be terrorized by terrorism.

The Federal Government responded by recognizing that this was a different kind of war with a different kind of enemy. We saw that this enemy used as a weapon the freedom and openness that Americans cherish but that it despises. We realize that our efforts to defend our Nation against this unconventional enemy were hampered by a lack of a unified strategy. To revisit a phrase that was used so often in the aftermath of September 11, we were not connecting

the dots. Turf battles, communication gaps, and interagency rivalries could no longer be tolerated. The stakes are simply too high.

The Department of Homeland Security whose budget we review here today is the single greatest manifestation of our efforts to create that unified strategy, to connect those dots, to coordinate an urgent new mission. This Committee played a key role in creating the Department. Indeed, we marked up and reported the authorizing legislation.

Having created the Department, we have also endeavored to help it succeed. We have confirmed eight highly talented and dedicated individuals, most notably the Secretary, who are leading the Department. We have conducted hearings and investigations on a wide range of homeland security issues, from the President's plan to better coordinate intelligence analysts and sharing, to unraveling the tangles of international terrorism financing, to protecting American agriculture from sabotage, to securing our vulnerable seaports. We have approved bills to reform the Department's multibillion dollar State grant program, to provide cutting-edge technology to first responders, to help the Department attract the talented individuals it needs with sought-after skills, and to ensure accountability within DHS's financial system.

The Department is now nearing the completion of its first year. Therefore, this budget is the first that can be reviewed in the context of actual performance and accomplishments. This Committee is its first stop on Capitol Hill. Indeed, the Secretary told me that he anticipates testifying some six times on the administration's budget.

I am pleased to note that under Secretary Ridge's dedicated leadership there have been many significant accomplishments. The melding of 22 Federal agencies with more than 170,000 employees has occurred with some of the resistance that we expected, but without the widespread turf battles that many predicted. The level of cooperation and coordination within this new Department, although certainly not perfect, is a vast improvement over the previous ad hoc structure. The initial focus on airport security has been expanded to include other vulnerabilities such as seaport security. Our first responders—the local and State emergency personnel on the front lines—are getting more funding, training, and guidance than ever before to carry out their vital missions.

Of course, there are some concerns. While our first responders have received more resources, the administration's budget includes a considerable cut in the basic State Homeland Security Grant Program. In addition, our States, communities, and first responders need a streamlined grant process that includes greater flexibility in how they can use Federal resources. While resource capabilities have improved, prevention lags. Advanced counterterrorism technologies have yet to reach the front lines in most cases.

While the addition of personnel at our ports of entry have brought us greater security at our borders, many smaller border communities in my State face new restrictions that have tremendously disrupted their day-to-day lives. And while our urban areas are receiving unprecedented Federal assistance, the concerns and vulnerabilities of our small cities, small towns, and small States

must not be overlooked. Perhaps more than any other area this one gets shortchanged in the administration's budget.

As the Department pursues programs to make our country more secure it is inevitable that a tension will arise between security and privacy. Americans treasure their civil liberties and expect their government to protect them wherever possible. Where privacy must be compromised in order to prevent terrorism, the government has an obligation to tell the American people clearly what information it is gathering and why it is necessary.

I am concerned about revelations that two airlines turned over passenger information to government agencies without any public notice or privacy safeguards. We simply cannot gain security if we lose trust. As the Department of Homeland Security develops its new passenger prescreening program, CAPS–II, it must be open and forthright with the American people so that we can determine whether the added security is worth the privacy costs. Programs such as this one must be crafted with care to minimize the impact on personal privacy and must be subject to close Congressional scrutiny. I know that the Department shares that goal.

The Department of Homeland Security's budget that we are examining today makes substantial investments in areas that are critical to our Nation's safety. I cannot say that I agree with each and every detail of the budget, particularly in the area of grants to States, communities and first responders, the Coast Guard, and port security. But I want to commend the Secretary for making tough choices in a lean budget year. I also want to recognize that when one looks at the President's budget overall that homeland security has clearly been made a top priority.

The war on terrorism is a different kind of war. We are proceeding to blaze a path in uncharted territory, making mistakes, getting a little lost, but then finding our way and making significant progress. I appreciate the difficulty of the mission assigned to the Department and I know that its leadership is committed to accomplishing that urgent mission without sacrificing the freedom and the openness our enemy seeks to destroy.

Senator Lieberman.

OPENING STATEMENT OF SENATOR LIEBERMAN

Senator LIEBERMAN. Thank you, Madam Chairman. May I say thank you first, for your characteristically gracious welcome. It is good to be back. I consider myself very fortunate to have had the opportunity I have had over the last year to be a presidential candidate and to take an extraordinary journey around this country. I learned a lot, including about the public's concern about homeland security, and I hope that will enable me to contribute even more constructively, hopefully, to these debates.

I cannot think of a better place to begin my reentry full-time to the Senate than at this Committee with you and my colleagues, or a better place than with you, Mr. Secretary, on this particular topic which is so critical to all that we are committed to doing here. I thank you very much again, Madam Chairman, for the good work you have been doing and for your very kind welcome back.

The fact is that we do meet here today with fresh evidence of the urgent need to secure our homeland. Last week information gath-

ered by intelligence services prompted the cancellation of several international flights to the United States. Deadly ricin was discovered in this building, right here in this building in Senator Frist's office. Obviously, we do not yet know the full implications of these incidents but we clearly do know more than enough to conclude that our Nation faces an array of threats from terrorists bent on doing terrible damage to us, and that we are still too vulnerable to their evil intentions.

A number of independent, nonpartisan expert commissions have sounded the alarm about our lack of adequate preparedness, and I am sure we are all concerned about the critical vulnerabilities that have yet to be adequately addressed.

Mr. Secretary, I believe that you have been given insufficient resources to do the job the Homeland Security Act requires you to do. The administration's fiscal year 2005 budget, which includes a stunning 30 percent cut government-wide for first responders, is the latest alarming evidence of shortchanging the homeland side of the war against terrorism. Our government and our Nation are still dangerously unprepared, as our former colleague Warren Rudman has said, to face the ongoing and very real threats of terrorism. We need far more funded and focused leadership to secure our domestic defenses and to fulfill the promise, the full promise, of the Homeland Security Act.

Have we made any progress in securing our homeland in the last year? Of course we have, and it is significant. We are surely safer now with the Department of Homeland Security than we were without it. We are certainly more aware of the threats we face and we now have a focal point for planning, implementing, and assessing our homeland security efforts.

We have improved airport and airline security. We have begun to look more critically at the millions of containers that enter our ports from abroad, including pushing the borders back to help secure containers before they reach American shores. We have begun to consolidate homeland defense work under one roof, and that is the agencies involved in homeland defense at the borders and elsewhere. And in science and technology we are starting to bring a new research and development agency to counter terrorists' threats into existence, although it still faces bureaucratic and funding constraints.

But we are clearly not as safe as we hoped we would be by now, more than 2 years after September 11 and a year after the Department was created. We are still without a strategy, an overall strategy as the Gilmore Commission pointed out, that sets priorities and deadlines for homeland security efforts and clearly allocates responsibilities among Federal agencies, State and local governments, and the private sector. The Homeland Security Act called for a robust intelligence fusion center within the Department of Homeland Security, but the administration created a separate threat center that I fear is without a clear home and stable funding and which does not truly break down the turf barriers among intelligence agencies.

The Homeland Security Act was intended to bring new leadership to transportation and port security, critical infrastructure protection, and bioterrorism preparedness. Yet the Federal effort in

each of these areas remains incomplete and in some cases confused. The Homeland Security Act was meant to provide adequate support to State and local governments and first responders. Here, too, the promise has not yet been kept as our vital State and local partners struggle to find the resources and guidance they need from the Federal Government.

Senator Collins has mentioned the three areas that I want to focus on myself and any concerned about shortchanging in the budget proposal of the administration, and that is to say, support for first responders, support for the preparedness, response, and prevention of bioterrorist acts, and port and container security, particularly the underfunding of the Coast Guard.

So I would say that we have a long way to go yet before we fulfill the promise we made to the American people, in those dark days following the September 11 terrorist attacks, to adequately secure our homeland. But I do want to stress that in my opinion these debates and discussions, even disagreements we have, are not and ought not to become partisan. They are disagreements of policy and priorities and in some cases of funding, in many cases of funding allocations. The fact is that we ought to aspire to achieve the same standard of non-partisanship in matters of homeland security that at our best we have achieved in matters of international security.

I certainly return to the Senate full-time with a commitment, Mr. Secretary, to work with you on that. The fact is that—with the creation of the Department and the appointment of Governor Ridge as Secretary—we have something very important, a new reality, which is an authorized and accountable member of the President's Cabinet, with whom Members of Congress and the public can discuss these critical matters. I look forward to doing so with you today and in the months ahead, Mr. Secretary, with the aim of achieving the goals that I know we have. I know that you agree with all of us that we have no more urgent priority in fulfilling our constitutional responsibilities to provide for the common defense and ensure domestic tranquility than to secure our homeland and the American people from terrorist attacks. Thank you very much.

Chairman COLLINS. Thank you, Senator. Senator Sununu.

Senator SUNUNU. Thank you, Madam Chair. I will defer to the Secretary and submit any formal testimony to the record.

Chairman COLLINS. Thank you. Senator Levin

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Madam Chairman, I will be very brief. First let me join you in welcoming back Senator Lieberman. In addition to supporting your comments, let me say that it was really in this room that Senator Lieberman was one of the key legislative creators of the Homeland Security Department. His initiative led to the very creation of the Department which Secretary Ridge leads and you literally would not be here today but for the fact that Senator Lieberman and a few others, but mainly Senator Lieberman, took the lead in creating a critically important department and in pulling together all of the departments, or most of them that are involved in protecting our homeland.

I also want to thank you, Secretary Ridge, for your visit to Michigan. You visited a community which is one of those smaller towns,

or smaller cities perhaps more accurately, and one of our counties which fit into the category which our Chairman talked about. Our grant programs do not adequately address the vulnerabilities that some of those communities at least have, particularly the one in Port Huron and St. Clair County that you visited. We are very appreciative of that visit. It made a great difference to them and I think will have an impact on the design overall of programs as you go along.

I also am deeply concerned about the cuts in the programs. There is an $800 million proposed cut in this budget for the Office of Domestic Preparedness. Further, our principal first responder program, the State Homeland Security Grant Program will be cut by almost $1 billion. That is deeply troubling. The Firefighter Assistance Grant Program is proposed for a 33 percent cut from the fiscal 2004 levels. I do not think that is anywhere near acceptable given the needs and the commitments which we made to our firefighters after September 11.

We also have to address the significant border problems that we have in this country, including the containers that come in and, Mr. Secretary, I know you are familiar with those nationwide and you saw firsthand the existence of those issues in my home State of Michigan.

I want to just focus quickly on two other issues. One is the need that we have, and Senator Lieberman mentioned this, to define the roles of our intelligence organizations, ones that analyze our intelligence. We have a number of entities that are involved in the analysis of intelligence. We have the Terrorist Threat Integration Center, we have a Counterterrorism Center at the CIA, we have the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, we have one in the FBI.

Senator Collins and I wrote Director Mueller, you Secretary Ridge, the Director of the Terrorist Threat Integration Center at the CIA Mr. Brennan, and the head of the CIA Mr. Tenet about these four entities that exist that relate and are supposed to be putting together in one place the information that we have relative to terrorist threats. We cannot divide, diffuse, confuse the responsibility of our key counterterrorism agencies. It has got to be located in one place. We have a whole commission now, the September 11 commission, that is looking at the failures of intelligence analysis prior to September 11.

Senator Collins and I have asked in this October 30 letter again, this is now a year after the first request that we made, for a statement as to what are the responsibilities of those four agencies, to avoid any overlap, any confusion, any kind of uncertainty as to who has the principal responsibility for analyzing terrorist threats, the intelligence relating to terrorists threats. We have to eliminate those turf barriers that exist that Senator Lieberman referred to. We have still not received a response to that October 30 letter. You were only one of the addressees and I would ask again that you accomplish that with your colleagues in the CIA and at the FBI.

I would ask that the balance of my statement, Madam Chairman, be placed in the record.

[The prepared opening statement of Senator Levin with attachments follows:]

PREPARED OPENING STATEMENT OF SENATOR LEVIN

Thank you very much Madam Chairman. I join you in welcoming Secretary Ridge once again to testify before this Committee and want to thank the Secretary for taking the time a few weeks ago to travel to Michigan and see first hand some of the unique homeland security challenges facing St. Clair County and Port Huron. I commend the Secretary for his commitment to strengthening our homeland security efforts and improving the programs that fund our domestic preparedness and response capabilities, protect our borders and ports and improve our transportation security.

Maintaining an adequate level of funding for first responders is critical to protecting our country from a terrorist attack and ensuring that we are able to adequately respond should such an attack occur. I am concerned about how this budget treats those on the front lines of our battle against terrorism, our first responders. Under this proposed budget for Fiscal Year 2005, the Office for Domestic Preparedness (ODP), which administers grant programs to assist State and local first responders, will receive $800 million *less* than it receive din FY04. One of the biggest ODP grant programs, the State Homeland Security Grant Program, will be cut by $1 billion. We cannot shortchange our first responders by cutting this vital funding and I will work with my colleagues to restore it.

While I am disappointed by these funding levels, I am pleased that the Department of Homeland Security appears to be moving away from the current small state funding formula. For example, using the .75 percent base for State Homeland Security Grant Program grants in FY 2004, Texas will received $4.04 per capita, whereas Wyoming will receive $28.72 per capita. The result is that while Texas has 42 times the population of Wyoming, it receives approximately one seventh of what Wyoming receives per capita. The consequence of the current .75 percent formula is that states with smaller populations receive far more, per capita, than more populated states, regardless of vulnerability of infrastructure or threat.

I am also concerned that this budget provides no funds for grants to enhance interoperability, even though ti remains one of the top priorities of our first responders, and cuts funding for the Emergency Management Performance Grant (EMPG) program by $10 million. Further, under this proposed budget, funding for the Firefighter Assistance Grant program is cut by $250 million, or 33 percent, from FY04 levels. This grant program was created by Congress in order to meet the basic, critical needs of the firefighting community. Thousands of firefighting personnel in Michigan and throughout the country rely on the Assistance to Firefighters Grant Program for the training, firefighting equipment, protective gear, and prevention programs that keep our citizens safe. Some of our fire departments in Michigan have to work with old and inefficient equipment such as corroding fire trucks with mechanical problems, and old water tanks unable to maintain necessary pressure levels to fight fires. Under the Administration's proposal, funding may not be available to these fire departments for their basic firefighting needs.

The DHS budget proposal notes that allocating grant funds within the Department will be coordinated with relevant preparedness programs in the Department of Justice. However, that Department has also cut funding for our first responders. The President's budget proposes massive cuts to local law enforcement programs that, if enacted, would severely compromise the safety of communities around the country. Not only are cops on the beat essential for maintaining community safety, but they are the first line of defense against potential terrorist attacks. The President's budget proposes a more than $650 million cut in funding for the COPS program, including a 100 percent cut in the COPS hiring program that helps local law enforcement meet demands for additional officers. On top of the COPS cuts, the President's budget eliminates funding for the local law enforcement block grant program (FY 2004 $235 million) and the Byrne grant program (FY 2004 $674 million). All of these programs provide vital funding to our first responders and it puzzles me as to why they would be diminished at a time when we are at an increased threat level.

Another issue that we need to address is our border protection. Southeast Michigan is home to five international border crossings. More than 40 percent of all U.S./Canada trade passes through Michigan/Ontario borders. The Ambassador Bridge is the busiest commercial crossing in North America and the Detroit-Windsor Tunnel is the busiest passenger vehicle tunnel on the northern border. The bridge facilitates approximately 25 percent of all trade between the U.S. and Canada. In 2003, there were over 3 million vehicle traffic crossings at the Ambassador Bridge—total value of goods ranging from $120–$130 billion. It is a most critical instrument in facilitating the U.S./Canadian Trade Agreement. Unnecessary and lengthy delays have seriously impacted our economic stability on both sides of the bridge. Effective and

secure functioning at this border crossing must be a priority consideration for this committee. We have seen improved and more secure commercial traffic flow at the Ambassador Bridge with the increased numbers of inspectors at our northern borders and with the implementation of NEXUS and FAST, two advanced technology and effective pre-screening programs. While border staffing levels have increased at our northern border crossings, increased border security requirements will add to longer processing times and additional staffing is needed. Our economy, which is increasingly dependent on just in time delivery, cannot afford delays at our borders.

Reverse inspections is a critical component of securing our port and bridge. Vehicles should not be allowed to enter the bridge without having cleared cargo inspections reducing potential for a terrorist act which would destroy the bridge and severely impact the economy of both the U.S. and Canada. The Legislation which calls for a pilot program on reverse inspections was passed in 2003, however it has not yet been put in place. If the Administration is serious about homeland security, it should implement reverse inspection without delay.

I am also concerned that the Department of Homeland Security has not yet reported to Congress on the plan for consolidating and co-locating Department of Homeland Security regional offices. Section 706 of the Homeland Security Act requires DHS to submit a consolidation plan to Congress no later than one year after the enactment of the Act (which was November 25, 2003). These decisions by DHS will impact my home state of Michigan because we are asking DHS to consider locating a first responder training facility, as well as a regional headquarters for DHS, in Michigan. As the Secretary is aware, two Michigan National Guard facilities, the Alpena Combat Readiness Training Center (CRTC) and Camp Grayling, are ideally suited to serve together as a training center for first responders. These state-of-the-art facilities currently train members of the active duty military, National Guard and first responders. Annually thousands of individuals from throughout the nation train at Alpena CRTC and Camp Grayling. For decades these sites have worked to expand their capacity and hone their training techniques. These investments have led to the creation of world class training facilities that would be ideally suited for training DHS staff and first responders from throughout the nation. In addition, Selfridge Air National Guard Base is being considered as a regional headquarters for DHS. This world class facility which currently is home to all five branches of our nation's military as well as FAA and Customs officials, would be ideally suited for such a purpose. I would urge the Department to complete this plan as soon as possible, and clarify its intent about working with Congress on these matters, so that we can begin to plan where these regional training centers will be located.

I would also like to briefly discuss the intelligence analysis mechanisms and strategies that exist within the Department of Homeland Security and outside of it. We all agree that intelligence is crucial to our national security. As we have seen, intelligence decisions can alter our country's political course. Because of that, it is absolutely essential for us to do everything in our power to ensure that our intelligence is credible. Over the last two years, many of us have been asking questions about the Administration's intelligence gathering capabilities and responsibilities. We have not received satisfactory answers to those questions. As I see it, part of the problem stems from the fact that our intelligence analysis has multiple branches, including the Terrorist Threat Integration Center (TTIC), the CIA's Counter Terrorism Center (CTC) and the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate. Although I have been asking for over a year, the Administration has yet to define how these three intelligence entities are duplicating one another or complementing one another. It is the responsibility of our current Administration to define the roles of the intelligence organizations. If the Administration cannot define the purposes of these entities, how can the people working at these agencies understand communication protocol and agency purpose and mission? Why should we feel safe when the employees and agencies tasked with gathering and disseminating intelligence are not entirely sure what they should be doing and to whom they should be talking? Chairman Collins and I wrote to the CIA last year asking for a comprehensive description of these three entitles. The explanation we received was completely unsatisfactory, so we wrote again to the DHS, CIA, and TTIC and requested an answer by November of last year. We are still waiting for a response. I would like to submit the correspondence pertaining to this subject into the record.

I look forward to discussing all of these issues in greater detail. I have outlined the general issues that I hope you will address. I realize that there are a lot of challenges facing the Department, however providing our first responders with the training and equipment they need must remain one of our highest priorities. I look forward to working with you and your staff on these very important issues.

SUSAN M. COLLINS, MAINE, CHAIRMAN

TED STEVENS, ALASKA
GEORGE V. VOINOVICH, OHIO
NORM COLEMAN, MINNESOTA
ARLEN SPECTER, PENNSYLVANIA
ROBERT F. BENNETT, UTAH
PETER G. FITZGERALD, ILLINOIS
JOHN E. SUNUNU, NEW HAMPSHIRE
RICHARD C. SHELBY, ALABAMA

JOSEPH I. LIEBERMAN, CONNECTICUT
CARL LEVIN, MICHIGAN
DANIEL K. AKAKA, HAWAII
RICHARD J. DURBIN, ILLINOIS
THOMAS R. CARPER, DELAWARE
MARK DAYTON, MINNESOTA
FRANK LAUTENBERG, NEW JERSEY
MARK PRYOR, ARKANSAS

MICHAEL D. BOPP, STAFF DIRECTOR AND CHIEF COUNSEL
JOYCE A. RECHTSCHAFFEN, MINORITY STAFF DIRECTOR AND COUNSEL

United States Senate

COMMITTEE ON
GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510-6250

September 15, 2003

Winston P. Wiley
Associate Director of Central Intelligence
for Homeland Security
Central Intelligence Agency
Washington, D.C. 20505

Dear Mr. Wiley:

On February 26, 2003, you testified before the Governmental Affairs Committee regarding the Terrorist Threat Integration Center (TTIC). The hearing focused on the consolidation of intelligence analyses; however, there seemed to be confusion among the witnesses as to the actual responsibilities of the various intelligence entities. At that hearing, Senator Levin requested that you prepare a statement on which entities in the federal government would have the primary responsibility for analyzing foreign intelligence and domestic intelligence, and how those entities would interact with the newly formed TTIC. Senator Collins seconded Senator Levin's request, and asked that such a statement include a description of the responsibilities of the FBI Counterterrorism Division, the CIA Counter Terrorist Center, and the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate in relation to the TTIC.

Our request raises fundamental questions about the operations of the TTIC and its interaction with other government agencies. The Committee has still not received the requested statement. It is our understanding that the CIA has been working on such a statement, but that it is still not complete.

It is vitally important that the responsibilities for the collection and analysis of intelligence be clearly assigned among the relevant agencies in the Intelligence Community, and that the division of responsibilities be understood by the Intelligence Community and by Congress. We ask that the statement we first requested at the February 26 hearing be provided to the Committee by October 1st. Thank you for your cooperation.

Sincerely,

Susan Collins

Susan M. Collins
Chairman

Carl Levin

Carl Levin
U.S. Senator

DIRECTOR
TERRORIST THREAT INTEGRATION CENTER
Washington DC 20505

7 October 2003

The Honorable Susan M. Collins
Chairman
United States Senate
Committee on Governmental Affairs
Washington, D.C. 20510-6250

Dear Chairman Collins:

Enclosed is a response to the transcript request submitted to Winston Wiley, the former Associate Director of Central Intelligence for Homeland Security, following the hearing held on 26 February 2003 regarding "Consolidating Intelligence Analysis: A Review of the President's Proposal to Create a Terrorist Threat Integration Center."

If you have any questions regarding the response, please contact Jack Dempsey, Office of Congressional Affairs, at 703-482-8802.

A copy of this letter (with enclosure) has also been provided to the Ranking Member of the Governmental Affairs Committee.

Sincerely,

John O. Brennan

Enclosure

Terrorist Threat Integration Center
Response to Senators Levin/Collins Transcript Request
From the 26 February 2003 Open Hearing
Senate Governmental Affairs Committee

Transcript Request:

Senator Collins: "I would second, as Chairman of the Committee, Senator Levin's request in this regard. I do think we need more definition on who is going to do what. The Department of Homeland Security's underlying law calls for it to analyze. That is part of the law. So I do believe we need more definition. I do recognize that the center is a work in progress, but I would ask the witnesses to **come back to us with a document that would define with more specificity the responsibilities of the components and the existing--the Counterterrorism Division at the FBI, the Counterterrorism Center at the CIA, the information analysis directorate at Homeland Security. I would like to see more definition in defining the responsibilities of those three units and how the new center interacts.** The goal is fusion not confusion. But when I look at the chart and plot the new center in, I am concerned about duplication, accountability, and responsibility. So I hope as you further work out the details of the center you would get back to us." ..." *(pp.62-63, Senate Committee on Governmental Affairs, February 26, 2003 open hearing on "Consolidating Intelligence Analysis: Review of the President's Proposal to Create TTIC.")*

Response: The Terrorist Threat Integration Center (TTIC) is currently working collaboratively across the Federal government to integrate terrorism information and analysis to provide a comprehensive, all-source-based picture of potential terrorist threats to U.S. interests. In this regard, TTIC works closely with the FBI's Counterterrorism Division, DHS's Information Analysis and Infrastructure Protection directorate, the DCI's Counterterrorism Center, and the Defense Intelligence Agency's Joint Intelligence Task Force--Counterterrorism, among others. In fact, all of these organizations are represented in TTIC and work together, on a daily business, to carry out the mission of their parent organization as well as that assigned to TTIC by the President: to enable the full integration of U.S. Government terrorist threat-related information and analysis, collected domestically or abroad.

As a relatively new entity, and one that is unique in the federal constellation, misperceptions are still common. One common misperception is that TTIC is a part of the Central Intelligence Agency. In actual fact, TTIC does not belong to any department or agency. It is a multi-agency joint venture composed of partner organizations including the Departments of Justice/Federal Bureau of Investigation, Homeland Security, Defense, and State, and the Central Intelligence Agency. TTIC reports to the Director of Central Intelligence, but in his statutory capacity as the head of the Intelligence Community. TTIC does not engage in any collection activities and it does not engage in operations of any kind. Unlike the FBI's Counterterrorism Division, the DCI's Counterterrorism Center, and the Department of Homeland Security, all of which have an operational or collection element, TTIC is focused on integrating and analyzing terrorist threat-related information collected domestically or abroad. We defer to these other organizations to provide you a full explanation of their roles and responsibilities.

While TTIC is still in its infancy, there is tangible evidence of the value of 'jointness,' as embodied in the TTIC construct, and TTIC is making a difference in the war against terrorism. For example, TTIC analysis has contributed to informed decision making within DHS about the appropriate threat level for the nation. The TTIC-maintained terrorist identities database informs the national watchlisting process and according to the Homeland Security Presidential Directive-6, will soon serve as the single source of international terrorist identities information for the newly established Terrorist Screening Center. In addition, the TTIC-hosted joint information sharing program office is actively implementing the Information Sharing Memorandum of Understanding signed in March 2003 by Attorney General Ashcroft, Secretary Ridge, and the Director of Central Intelligence. Under the auspices of this program office, business processes are being re-engineered to facilitate the flow of information throughout the federal government, but in particular, to the Department of Homeland Security. Specific issues being addressed at this time include establishing standards for tear lines, reaching out to non-Intelligence Community federal departments and agencies, and rethinking reporting standards.

As the national approach to combating terrorism and protecting the homeland evolves, TTIC will continue to carry out the mission assigned to it by the President: to enable the full integration of U.S. Government terrorist threat-related information and analysis, collected domestically and abroad - and TTIC will fulfill its mission in full coordination with partner organizations including the Department of Homeland Security, the Federal Bureau of Investigation, the Central Intelligence Agency, the Department of Defense, and the Department of State. We will keep you informed of our progress.

SUSAN M. COLLINS, MAINE, CHAIRMAN

TED STEVENS, ALASKA
GEORGE V. VOINOVICH, OHIO
NORM COLEMAN, MINNESOTA
ARLEN SPECTER, PENNSYLVANIA
ROBERT F. BENNETT, UTAH
PETER G. FITZGERALD, ILLINOIS
JOHN E. SUNUNU, NEW HAMPSHIRE
RICHARD C. SHELBY, ALABAMA

JOSEPH I. LIEBERMAN, CONNECTICUT
CARL LEVIN, MICHIGAN
DANIEL K. AKAKA, HAWAII
RICHARD J. DURBIN, ILLINOIS
THOMAS R. CARPER, DELAWARE
MARK DAYTON, MINNESOTA
FRANK LAUTENBERG, NEW JERSEY
MARK PRYOR, ARKANSAS

MICHAEL D. COPPS, STAFF DIRECTOR AND CHIEF COUNSEL
JOYCE A. RECHTSCHAFFEN, MINORITY STAFF DIRECTOR AND COUNSEL

United States Senate

COMMITTEE ON
GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510-6250

October 30, 2003

The Honorable Robert S. Mueller III
Director
Federal Bureau of Investigation
Washington, D.C. 20535

The Honorable George J. Tenet
Director of Central Intelligence
Washington, D.C. 20505

The Honorable Tom Ridge
Secretary
Department of Homeland Security
Washington, D.C. 20528

John O. Brennan
Director
Terrorist Threat Integration Center
Washington, D.C. 20505

Dear Sirs:

On February 26, 2003, the Governmental Affairs Committee held its second day of hearings regarding the creation of the Terrorist Threat Integration Center, and heard testimony from witnesses from the Federal Bureau of Investigation, Central Intelligence Agency, and the Department of Homeland Security. The hearing raised questions about the structure of the TTIC, and near the close of the hearing, we asked the panel for further information regarding the division of responsibility among key counterterrorism agencies. Specifically, we asked which agencies would have the primary responsibility for analyzing foreign intelligence and domestic intelligence, what relationship the TTIC would have with those agencies, and for a thorough discussion of the responsibilities of the FBI's Counterterrorism Division, the CIA's Counter Terrorist Center, and the Information Analysis and Infrastructure Protection Directorate of DHS in light of TTIC's creation.

On October 7, 2003, we received a response from Mr. Brennan, Director of TTIC, which purported to address some of the questions posed at the hearing. However, the response did not provide much of the information requested at the hearing, despite the fact that it took more than seven months to prepare. As we indicated at the hearing in February, it is critical that there be clear lines of responsibility in the analysis of intelligence, and that these responsibilities be understood by all of the agencies involved in our counterterrorism efforts. Since this Committee's hearings in February, concerns about the TTIC's role have only grown.

Given the incomplete nature of the October 7 response, we pose the following questions to each of you, and request that you provide a written response by November 14, 2003.

- Please describe which component of the U.S. Intelligence Community has the primary responsibility for the analysis of foreign intelligence relating to terrorism. If the response is not TTIC, describe how this agency's responsibilities relate to the TTIC's responsibilities.

- Please describe which component of the U.S. Intelligence Community has the primary responsibility for the analysis of domestic intelligence relating to terrorism. Describe how this agency's responsibilities relate to the TTIC's responsibilities.

- Please describe the responsibilities of the Counterterrorism Division of the FBI as they relate to the analysis of terrorism-related intelligence. Describe how the Counterterrorism Division's responsibilities differ from, and relate to, the TTIC's responsibilities.

- Please describe the responsibilities of the Counter Terrorist Center as they relate to the analysis of terrorism-related intelligence. Describe how the Counter Terrorist Center's responsibilities differ from, and relate to, the TTIC's responsibilities.

- Please describe the responsibilities of the IAIP Directorate of DHS as they relate to the analysis of terrorism-related intelligence. Describe how IAIP's responsibilities differ from, and relate to, the TTIC's responsibilities.

If you have any questions about this matter, please have your staff contact David Kass with Senator Collins at 202-224-4751, or Laura Stuber with Senator Levin at 202-224-9505.

Sincerely,

Susan Collins

Susan M. Collins
Chairman

Carl Levin
U.S. Senator

Chairman COLLINS. Thank you, Senator. Senator Akaka.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Madam Chairman. Secretary Ridge, it is a real pleasure to have you before us today. There was never any doubt in my mind as to how hard it would be to create a new agency, but I want you to know that I saw you as the right person for the job.

Secretary RIDGE. Thank you, Senator

Senator AKAKA. I have a longer statement, Madam Chairman, and I ask that it be made part of the record.

Chairman COLLINS. Without objection.

[The prepared opening statement of Senator Akaka follows:]

PREPARED OPENING STATEMENT OF SENATOR AKAKA

Thank you Madam Chairman. Secretary Ridge, it is a pleasure to have you before us once again. There was never any doubt as to how hard it would be to create a new agency, but I saw you as the right person for this job.

Today you may hear me focus on the problems of this new department, on my perception that the glass is less than half full, but I want you to know that I still believe that you are the right man for this difficult task.

When the Department of Homeland Security (DHS) was created, we knew it would take time to meld so many previously independent or otherwise affiliated agencies, bureaus, and offices into a single unit. But, all of us were also aware of the importance of quickly ensuring that these newly merged component parts operate as one cohesive and effective system to protect our country.

The urgency of achieving that end-state has not diminished and, in fact, becomes more acute with each passing day. And yet, Mr. Secretary, the Committee hears that DHS coordination and operation efficiency is hampered by functional and cultural differences, and it appears to me that the administration's budget proposal fails to provide sufficient funds to implement critical functions of the Department.

The President's budget calls for $47.4 billion for the Department, of which 32 percent is for non-homeland security activities. While the main mission of the Department is to fight and deter attacks against the nation, the legacy agencies transferred to DHS have many non-homeland security missions that Americans rely upon and which remain integral to the agencies' functional capabilities. We must make sure that these non-homeland security missions and functions are not short-changed.

For example, items identified as non-homeland security programs include first responder grants, disaster mitigation, firefighter grants, the disaster assistance direct loan program, mitigation grants, flood map modernization, the radiological emergency preparedness program, and emergency management performance grants.

From the President's budget, it appears that the designation of a program as either homeland security or non-homeland security is critical to the amount of funding a program receives. Yet, it is unclear why or how the Department designated some as security-related and others not.

I am also concerned about the level of support being provided to the states. For example, states are facing critical challenges in making communications interoperable, yet SAFECOM, which provides public safety agencies the guidance to achieve interoperable communications, does not have a specific funding level in the budget. States face funding shortfalls to secure seaports, yet the budget does not include funding for port security grants.

The proposed budget cuts funding for non-intrusive detection technology, technical assistance with emergency response planning, and first responder training.

In addition, in some areas, budget reductions seem to be responsible for delaying critical preparedness programs. For example, there are a series of goals under Emergency Preparedness and Response that list FY 2009 as their target completion date. These include requiring that all state, tribal, and county jurisdictions complete self-assessments of their ability to recover from terrorist attacks or other disasters. These assessments should not take so long to complete, but the National Emergency Management Baseline Capability Assessment Program has been cut by $227 million.

The President's budget request falls short of protecting homeland security for all states. Formula grant funding, which protects smaller states, has been reduced in

the budget request by 59 percent. The President's request eliminates minimum funding levels established by Congress to protect smaller states. Instead, the budget request requires that formula based grants be allocated according to population, critical infrastructure, and other factors determined by the Secretary. This proposal threatens to harm all states by structurally changing homeland security grant funding according to a yet to be determined formula.

Critical to the integration and smooth functioning of the Department is the new human resources system, which is currently being developed. DHS, along with the Department of Defense, is part of the most massive transformation of government since 1947. I am concerned that this is occurring without sufficient funding to maintain these new personnel systems and without rationalizing agency missions to personnel needs. In the 1990s, agency staffing was cut without giving sufficient consideration to what employees do. The present administration is cutting agency budgets without knowing what agencies do, forcing these agencies to do more with less, and imposing rigid performance rules without credible transparent and accountable systems in place.

We must ensure that agencies have the funding necessary to manage their workforce effectively—including funding for overall management training, bonuses, and other recruitment and retention programs, such as student loan repayment programs.

As I review the President's budget submission, I am disturbed by what appears to be a trend in cuts to human capital and management functions. The Department is requesting $133.5 million for a new human resource system, declaring it to be an investment in human capital, while at the same time making cuts in human captial areas that are essential to the long term security of our nation. For example, the Science and Technology Directorate has cut its FY05 funding for university and fellowship programs by $38.8 million. This could lead to a less prepared future work force if fewer new people are being trained and recruited through these programs.

It is important that DHS remain committed to developing and maintaining the most innovative and skilled technical staff possible. The United States should lead the world in the development of technology and science applications to thwart terrorism both domestically and internationally. I am concerned that budget cuts to a program, like the university and fellowship programs, may undermine our ability to recruit and train new Federal workers in these critical areas.

The Department may be robbing Peter to pay Paul. An example is in the Information Analysis and Infrastructure Protection Directorate where a net increase in the number of intelligence analysts has been accomplished by reducing the number of policy and program professional staff by eleven. Perhaps this is a change in name only, but my concern is that a large reduction in policy and program analysts could led to the development of technical programs that are not well-coordinated or well-thought out.

DHS should be mindful of the effect of cutting a disproportionate number of policy and program professional staff. I am concerned that these actions could lead to the development of technical programs that are not well-coordinated or to the failure to develop needed programs.

Steps should be taken to ensure that the loss of these positions in the Information Analysis and Infrastructure Protection Directorate does not interfere with the very important mission of assessing threats and providing coordinated recommendations for a response.

There also needs to be significant funding for some of the critical management functions, including the internal oversight mechanisms, such as the Inspector General, the Privacy Officer, and the Civil Rights and Civil Liberties Office, that were put in place by the Congress to ensure that we do not erode our liberties and freedoms when fighting terrorism. Moreover, the Secretary's office contains the responsibility under the Chief Information Officer to develop a comprehensive data management plan essential for first responders. But, to date, the Department has been unable to acquire the geospatial data, such as critical infrastructure, street mapping, first responder locations, and government facilities, necessary to build a repository of information which could be shared throughout the Department and with state and local governments. Failure to achieve this common information database hampers prevention and planning for emergency response and recovery operations.

Last week the Senate had to close its offices because of a poison attack. Fortunately no one was injured. However, the attack illustrated the continuing vulnerability of our society to such dangers and should be a wake-up call to all of us that time is not on our side. It sometimes appears to me that more attention and more money is being devoted to developing a new personnel system in the Department of Homeland Security than to providing grants to states and developing the technologies that first responders will soon need against threats they cannot anticipate.

Madam Chairman thank you again for holding this hearing and thank you, Mr. Secretary, for being here. I look forward to your testimony and responses to our questions.

Senator AKAKA. I will just say now that when the Department of Homeland Security was created we knew it would take time to meld so many previously independent or otherwise affiliated agencies, bureaus, and offices into a single unit. But we were also aware of the importance of quickly ensuring that these newly merged component parts operate as one cohesive and effective system to protect our country.

The urgency of achieving that end state has not diminished, and in fact becomes more acute with each passing day. Yet, Mr. Secretary, the Committee hears that DHS coordination and operation efficiency is hampered by functional and cultural differences and it appears to me that the administration budget proposal fails to provide sufficient funds to implement critical functions of the Department.

The President's budget calls for $47.4 billion for the Department of which 32 percent is for Non-Homeland security activities. While the main mission of the Department is to fight and deter attacks against the Nation, the legacy agencies transferred to DHS have many non-homeland security missions that Americans rely upon which remain integral to the agency's functional capabilities. We must make sure that these non-homeland security missions and functions are not shortchanged.

From the President's budget it appears that the designation of a program as either homeland security or non-homeland security is critical to the amount of funding a program receives. Yet it is unclear why or how the Department designated some as security-related and others as not.

I am also concerned about the level of support being provided to the States. For example, States are facing critical challenges in making communications interoperable, yet SAFECOM, which provides public safety agencies the guidance to achieve interoperable communications does not have a specific funding level in the budget. States funding shortfalls to secure seaports, yet the budget does not include funding for port security grants.

Formula grant funding, which protects smaller States such as Hawaii and Maine, has been reduced in the budget request by 59 percent. The President's request eliminates minimum funding levels established by Congress to protect smaller States. This proposal threatens to harm all States by structurally changing homeland security grant funding according to a yet to be determined formula.

Critical to the integration and smooth functioning of the Department is a new human resources system which is near completion. DHS along with the Department of Defense is part of the most massive transformation of government since 1947. I am concerned that this is occurring without sufficient funding to maintain these new personnel systems and without rationalizing agency missions to personnel needs. We must ensure that agencies have the funding necessary to manage their workforce effectively, including funding for overall management training, bonuses, and other recruitment and retention programs such as student loan repayment programs.

As I review the President's budget submission, I am disturbed by what appears to be a trend in cuts to human capital and management functions. The department is requesting $133.5 million for a new human resource system, declaring it to be an investment in human capital while at the same time making cuts in human capital areas that are essential to the long-term security of our Nation.

For example, the Science and Technology Directorate has cut its fiscal year 2005 funding for university and fellowship programs by $38.8 million. This could lead to a less prepared future workforce if fewer new people are being trained and recruited to these programs. It is important that DHS remain committed to developing and maintaining the most innovative and skilled technical staff possible. The United States should lead the world in the development of technology and science applications to thwart terrorism both domestically and internationally. I am concerned that budget cuts to a program like the university and fellowship programs may undermine our ability to recruit and train new Federal workers in these critical areas.

Madam Chairman, thank you again for this hearing and thank you, Mr. Secretary, for being here.

Chairman COLLINS. Thank you, Senator. Senator Durbin.

OPENING STATEMENT OF SENATOR DURBIN

Senator DURBIN. Thanks, Madam Chairman.

Secretary Ridge, thank you for being here. From the announcement of your appointment to this day I continue to believe that you were the very best choice for this important position to defend America. I thank you for your public service and I thank you for your friendship.

Mr. Secretary, having said that, this administration's speeches say that we are in a pitched battle in a war on terrorism, but the budget that has been submitted suggests that major military operations in this war on terrorism are winding down exactly when we need them the most.

You have heard from my colleagues and I would like to make the same point which I think really goes to the heart of this issue. I am concerned this budget shortchanges our first line of defense, America's first responders in counties, cities, and communities. The budget calls for a 41 percent cut, nearly $1 billion for State and local grants in the Office of Domestic Preparedness. FIRE Act grants are cut by 33 percent, from $746 million appropriated for this year down to $500 million for fiscal year 2005. State and local training, exercises, and technical assistance funds face a projected 44 percent cut. While we appear to call for enhanced urban area security initiative funding, this budget reflects an 18 percent overall cut from the current year.

I know that it is not your bailiwick but in the same budget the President virtually eliminates the COPS program, a 91 percent cut from fiscal year 2003 funding level, and 85 percent cut from fiscal year 2004 funding level. In Illinois, during fiscal year 2003, COPS grants provided funding for 123 full-time police officers. A cut of 91 percent would be 111 fewer police officers patrolling Illinois' neighborhoods and schools.

Mr. Secretary, how can we win this war on terrorism with fewer soldiers, fewer brave men and women who are truly our first line of defense? Our political speeches will not save us. Our political promises will not protect us. We need to put our money where our security will be, on the front line. We cannot afford a hollow army in our war on terrorism.

Second, I have focused on one issue more than any other in this whole area and it has been the interoperability of our computers, our information technology. Starting September 11 and to this very moment I have tried to make this my issue because I believe it passionately, that unless and until the technology can communicate and the people are willing to share, we will not be as strong as we should be in our defense in the war on terrorism.

I asked for a Manhattan Project in the creation of your department. The administration opposed it. They said it is unnecessary. I thought that we had an opportunity to do something unique, to bring together all of the agencies dealing with the defense and security of our Nation into one common effort, one stronger effort. In June of last year your CIO Steve Cooper announced that, and I quote from an article published in *Computerworld,* "Steve Cooper, who is CIO at the U.S. Department of Homeland Security must untangle the mess of disparate networks' data standards of the 22 Federal agencies that merged to form the DHS. He said last week"—and this was in June of last year—"that a unified IT infrastructure will be completed within 18 to 24 months."

Mr. Secretary, we have to do better. You have the responsibility more than any other member of the cabinet to bring this together. I am concerned, too, when the President announces the creation by executive order of two new terrorist threat information gathering and analysis agencies, the Terrorist Threat Integration Center, not under your leadership, but under the CIA, and the Terrorist Screening Center, now part of the FBI. I am afraid that this will continue to perpetuate rivalries. It builds the stovepipes even higher.

The obvious question is, are you losing the turf battle within your own administration to bring this information technology together? Our confidence in our intelligence community has been shaken by the litany of inaccuracies and misleading statements leading up to the invasion of Iraq. We are now in the midst of a review called by the President of the United States, a commission to investigate what went wrong in most of the substantial intelligence failures in modern history in the United States. We cannot allow the same thing to happen when it comes to our domestic security.

You, more than any other person, have that responsibility to gather together these resources and forces to make certain that our intelligence makes America safer. I am looking forward to your testimony on the efforts that you are making.

Thank you, Madam Chairman.

Chairman COLLINS. Thank you. Senator Pryor.

OPENING STATEMENT OF SENATOR PRYOR

Senator PRYOR. Thank you, Madam Chairman. I just want to again welcome Secretary Ridge to this Committee. Appreciate your

public service and all that you have done in homeland security. My colleagues have covered some of the ground I wanted to cover, but Madam Chairman, I just want to thank you and also welcome Senator Lieberman back. He has been such a leader with regard to homeland security and it is so great to have you back here and have your mind on this. I look forward to hearing your thoughts as we progress in this hearing today.

Thank you, Madam Chairman.

Chairman COLLINS. Thank you. Mr. Secretary, we are pleased to have you here and we look forward to hearing your statement. You may proceed.

TESTIMONY OF HON. TOM RIDGE,[1] SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary RIDGE. Thank you. Madam Chairman, Senator Lieberman, and Members of the Committee, I am grateful for the opportunity to appear before you today and present the President's budget and priorities for the Department of Homeland Security in the coming year.

Before the tragic events of September 11, no single government entity had homeland security as its primary charge. With the creation of the Department of Homeland Security, and this Committee was there at its birth, that charge was given to us, 22 agencies, 180,000 employees brought together to pursue a single mission. That mission, to secure our Nation and citizens from the threats of terrorism and natural disaster, is one that does not change or lessen in importance with the passing of time. As several Senators have commented, the recent ricin scare serves as a difficult reminder that terrorism is a threat that we must confront each and every day with the same commitment and the same sense of urgency we all remember from the day our Nation was attacked 2 years ago.

Now as we prepare to celebrate our one-year anniversary as a Department, it is the steadfast support of this Congress and the resources you have provided that have made it possible for us to not only carry out a vigorous and ambitious slate of security initiatives, but also to say and to join with you as you have commented today, to say with confidence that Americans are indeed safer today. I am also mindful of the fact that we still have more work to do.

In a short time we have strengthened airline security, increased vigilance at our borders and ports, forged unprecedented partnerships across the private sector, State and local governments, improved information sharing, launched robust efforts to engage citizens in preparation efforts, and distributed funds and resources for our dedicated first responders. Of course, there is still more we can do and there is still more we must do. The President's budget request for the Department in fiscal year 2005 includes $40.2 billion in new resources, a 10 percent increase above the current year's level. This increase in funding will provide the resources we need to expand and improve existing projects and programs as well as build new barriers to terrorists who wish us harm.

[1] The prepared statement of Secretary Ridge appears in the Appendix on page 47.

Let me touch briefly on a couple of areas where specific increases in our resources will help us continue to make progress at our borders, in our skies, on our waterways, and throughout the Nation. To further strengthen our border and port security, this budget includes a $411 million increase for Customs and Border Protection, Immigration and Customs Enforcement, and Coast Guard.

This funding will support such innovative initiatives as the recently launched US–VISIT. This program is now operational at 115 airports and 14 seaports across the country to help ensure that our borders remain open to legitimate travel but closed to terrorists. That program has been very successful utilizing biometric technology to process more than 1 million legitimate passengers since the beginning of the year, and since the program began, we have matched 104 potential entrants against criminal watch lists. With additional funding of $340 million this year, we will continue to expand US–VISIT to include land borders and additional seaports.

However, we also recognize that potential enemies will not always arrive at a Customs checkpoint. That is why we have more than $64 million to enhance monitoring efforts along the border and between the ports. We have also requested an increase of $186 million to better enforce our immigration policies. We are also pushing our perimeter security outward, making sure that our borders are the last line of defense, not the first.

The Container Security Initiative, for example, focuses on prescreening cargo before it even reaches our ports, and for that matter before it is even loaded onto the ships. This budget includes $25 million in additional funding to enhance our presence at existing ports and to begin the final phase of the Container Security Initiative, especially in high-risk areas around the world.

Also the Coast Guard's budget will increase by 8 percent which includes funding for the continuation of the Integrated Deepwater System, and important new resources of more than $100 million to implement the Maritime Transportation Security Act.

One of the greatest areas of concern since September 11, of course, has been aviation security, and thus continues to be an area of high priority for Congress and for the administration and for this country. It is also a high priority within the budget with an increase of 20 percent this year. The Transportation Security Administration will receive an additional $890 million to continue to improve the quality and efficiency of the screening process. Also, considerable funds will be available to continue the research and deployment of air cargo screening technology as well as accelerate the development of technologies that can counter the threat of portable anti-aircraft missiles.

While we have seen the havoc possible when aircraft are used as weapons, we have yet to experience the full impact, and I emphasize the full impact of a bioterror attack, and may we never have to do so. But we must be prepared. It is in that spirit that Secretary Tommy Thompson and I announced a $274 million biosurveillance program initiative designed to protect the Nation against bioterrorism and to strengthen the public health infrastructure. The initiative will enhance ongoing surveillance programs for human health, hospitals, vaccines, food supply, State and local pre-

paredness, and environmental monitoring and integrate them into one comprehensive system.

In addition, one of our primary responsibilities is to gather intelligence and share information with the private sector and State and local officials as we work to secure the vast critical infrastructure upon which our economy and our way of life depends. That is why Information Analysis and Infrastructure Protection will receive in excess of $800 million in this budget, an increase in funding that will enable us to carry out this important task.

Finally, as I have said many times in the past, for the homeland to be secure, the hometown must be secure. That is why we continue to funnel resources to our State and local partners as well as to ensure that those who serve on the front lines of the new war, our firefighters, police, and medical personnel have everything they need. With that in mind, the total first responder funding in this budget adds another $3.5 billion to the more than $8 billion we have made available since March 1 of last year.

These are just some of our budget priorities over the coming year. Priorities that reflect the vast nature of our mission, whether safeguarding America from terrorist attack or providing aid in the face of natural disaster, our charge never changes and our course must never alter. To protect the people we serve is the greatest call of any government, and through the work of many, from those in Congress who allocate the resources to the governors and the mayors to those who work to fill gaps in their State and city security, and to a citizen who makes a preparedness kit, that call is being answered and embraced by the entire Nation.

I would like to thank this Committee and Members for their continued support of the Department's mission and our goal to make America stronger, safer, and better prepared every single day. I look forward to continuing to build this Department as we work together to secure a stronger and safer America.

Thank you.

Chairman COLLINS. Thank you, Mr. Secretary. We will now begin a round of 7-minute questions and answers.

Mr. Secretary, as a former governor you appreciate perhaps better than most people that State and local governments—regardless of their size—are incurring additional costs in this new era of homeland security. For example, according to the Portland, Maine police chief the city of Portland spends an additional $5,000 each week in extra police costs alone whenever the national terrorism alert increases to Code Orange. We have also recently seen in Maine a threat to the Casco Bay Bridge, which closed down the bridge, diverted Coast Guard, police, and fire resources, to deal with that threat. So regardless of the population of a State, every State has homeland security vulnerabilities and needs.

In previous testimony before this Committee and also the Appropriations Committee you indicated your recognition that every State needs a minimum amount of homeland security funding. Is that still your position?

Secretary RIDGE. Madam Chairman, I still believe that as we take a look at the ODP funding that is to be directed to the States and local governments, which also gives the Secretary, it gives me the flexibility to allocate more than just on population, that even

under those circumstances there should be a minimum allocated to individual States because there is still basic support of infrastructure that they need to build and sustain in order to create a national response capability.

Chairman COLLINS. This Committee held a hearing last year on the threat posed by agroterrorism, and I think that is another example where rural America faces a threat that is very difficult to deal with and is going to require increased coordination. That is another example of why we have to recognize that population does not automatically translate into vulnerabilities. Would you agree with that?

Secretary RIDGE. I would, Madam Chairman. One of the opportunities we have for the first time in the history of the Department, and I think for that matter for the first time since the country responded to September 11, is to build that infrastructure and allocate those monies according to strategic plans that governors have submitted.

As part of the requirement that we imposed on our partners at the State level, we asked the governors of the States and the territories to submit strategic security plans to us. They were all due by January 31 of this year so we could take a look at what they perceive to be the threats, their vulnerabilities, their critical infrastructure. Your point is well taken. So we could make a determination not based exclusively on population as to how these dollars should be allocated, and I look forward to working with this Committee, and Congress frankly, to appropriately use the flexibility that the language gives the Secretary to target these resources consistent with the State plans that we are getting from our colleagues in State Government.

Chairman COLLINS. I appreciate that assurance. As you know, the administration's budget does not appear to maintain the minimum for every State. It does give you some discretion and I have great faith in your exercise of that discretion. I also hope you will be Secretary forever. But in the event that does not happen, I am going to be working with my colleagues to clarify the language in the budget.

With regard to first responders, let me also commend you on your recent reorganization within the Department to streamline the homeland security grant process. Both Senator Levin and I have worked with you to try to have a single number, one-stop shopping if you will, for communities to be able to find out more easily what funds are available. I do have two concerns however. One, as I mentioned and several of us did in our opening statements, the funding for the State homeland security grant program is cut by nearly $2 billion compared to what was appropriated last year.

And second, I am still hearing complaints that the money is slow to get to first responders and to get to communities. I personally have concluded the Department is not at fault but that the States have not been as efficient in passing on the money as they should be. Could you comment on both of those issues, first of all the cut in the budget, and second, how can we ensure that the money is reaching those on the front lines as quickly as possible?

Secretary RIDGE. First of all, to put it in context, Madam Chairman, if just the dollars we have requested this year are appropriated by Congress, the amount of money to our first responders and State and local governments since fiscal year 2001 will be about $15 billion. So as we took a look at what we have been able to do with regard to first responders and other needs within this country, the allocation of those resources were made part of the budget that I submitted to OMB. As you well recall, last year we submitted a request for assistance to the fire companies at $500 million and Congress raised it. We did shift considerable resources from the State funding formula to the Urban Area Security Initiative because I think it is generally understood and, I think generally preferred, that as much of these dollars be distributed based on threat and risk.

Having said that, you and I also have had the conversation that we still need a certain amount going to the individual States to build up their own capacity to respond to the unpredictable nature of terrorism itself. But the bulk of dollars we believe should be distributed according to threat and risk. Now with the maturity and growth within the Department of the Information Analysis and Infrastructure Protection unit, with the strategic plans that are being developed by the States, and interaction between the Federal Government, the State Government and local governments I believe we can better target these resources.

Chairman COLLINS. Finally, I want you to address the Coast Guard budget. Senator Lieberman and I wrote to OMB last fall to urge that the Deepwater Program, which is a very comprehensive program to upgrade the Coast Guard's assets since it has so many aging cutters and aircraft. We had proposed funding deepwater over a 10-year period, which in the long run would actually save money for the Federal Government, significant money, as well as allow the Coast Guard to upgrade its fleet far more quickly.

This budget does include a commendable increase in the Coast Guard budget but it still funds the Deepwater Program over 22 years. Could you comment on what you think is the appropriate time for rebuilding the Coast Guard? We are concerned, given the Coast Guard's traditional missions and its vital homeland security missions that too many of its aircraft and cutters are being sidelined because of maintenance and aging problems.

Secretary RIDGE. Madam Chairman, first of all I think given the fiscal and security environment, the increase to the Coast Guard, nearly an 8 percent increase, again as we set priorities within the Department is precisely where we think we need to be. If the fiscal environment changes, security environment potentially changes, there may be some alterations to that. But again, we are quite aware of the fact that we have cutters that need repair and that their maintenance costs continue to increase because of the age of some of this equipment. But we are quite comfortable, given the nearly $500 million that we requested the Congress to appropriate, that we will continue to maintain the same level of service in both the homeland security and the non-homeland security areas.

We also asked you for additional revenue for Rescue 21, which is a part of the international distress system. In this program, additional money for maritime safety and security teams, which you

give. You give us another $100 million to assist us in dealing with the challenges of developing a maritime transportation strategy and to do the inspection of ports as well as vessels.

So again, in the fiscal environment, in the security environment, we have asked for more. You have given us more and we will continue to maintain the same level of service both in homeland and non-homeland functions.

Chairman COLLINS. Thank you. Senator Lieberman.

Senator LIEBERMAN. Thanks, Madam Chairman.

Mr. Secretary, let me just follow up, because Senator Collins and I do share this concern about port security and the funding of the Coast Guard. If I read this budget proposal of the administration correctly, with regard to the modernization of the Coast Guard fleet we are on a schedule where it will take 22 years to achieve that modernization. In the midst of the extraordinary increase in responsibilities that the Coast Guard has taken on ably with regard to homeland security, how can we justify not putting more into their fleet more quickly? To wait 22 years for them to achieve the level of modernization that they say they need, and which I believe they do need, seems much too long and really unrealistic and unacceptable.

Secretary RIDGE. Senator, the Congress has supported the levels that the administration has requested, and as you know, the Coast Guard is probably as effective an agency for taking every single cent that they get and maximizing its use. As we took a look at our strategic needs with regard to homeland security as well as fiscal concerns that legitimately should be imposed on all of government including the Department of Homeland Security, the balancing of the fiscal and security environment, we requested more money, additional funds for rescue, a little bit more money for the Deepwater Program, a few more additional dollars to implement the Maritime Transportation Security Act, and for fiscal year 2005 believe that is the appropriate balance.

At sometime in the future, depending on circumstances, if there is an opportunity to significantly increase or accelerate the modernization of the fleet—but we are not going to do anything to jeopardize the safety of those who operate the fleet or to minimize or denigrate our mission—we believe these dollars substantially will get us through 2005, maintaining and in some areas increasing the capacity we have to provide Coast Guard services to support homeland security function but also increasing the capacity to deal with the non-homeland security requirements as well.

Senator LIEBERMAN. I hope that we in Congress, again on a bipartisan basis, can put more money into this Deepwater Program of the Coast Guard to modernize their fleet. Some of us on the Committee serve on the Armed Services Committee as well and while the amount of money put into this fleet modernization program for the Coast Guard is not insignificant, it truly does pale in comparison to the billions of dollars we are putting into other programs through the Department of Defense. I do think we have got to start to look at Coast Guard capital needs in the same way we do the services, so I hope we can turn that around here.

I want to go now to bioterrorism. I noted that on January 29, as you mentioned, Secretary Thompson and yourself held a press con-

ference announcing this $274 million program to improve our Nation's bioterrorism surveillance capabilities. I believe that is critically important and I applaud you for that. As a matter of fact, in one of the hearings that I was privileged to chair of this Committee shortly after September 11, this need was focused on.

But I am concerned as I look at the budget details that it appears that a lot of the funding for this surveillance program that you have announced comes from cannibalizing existing bioterrorism programs, and the most unacceptable act of cannibalization to me is the cut, the $105 million cut, in bioterrorism preparedness grants to State and local health departments, which again are our first line of defense, first responders. The administration is also cutting another $39 million in grants which were to have developed hospital surge capacity to respond to a bioterrorism attack. Those are the very programs that the Health and Human Services official in charge of terrorism preparedness had said should be increased. Indeed one public health official said that the administration's budget proposals on bioterrorism were like, "laying off firefighters while investing in new hoses and ladders."

So obviously I want to ask you who in the administration sets these priorities? Good move on bioterrorism surveillance but wrong place to get the money, by cutting these two other critically important programs.

Secretary RIDGE. First of all, Senator, I think if my recollection is correct a year or two ago the Congress acted quite aggressively and quite generously with bioterrorism grants to State and local governments. I do not recall the figure but I think it was an excess of $1.2 billion or $1.3 billion. And there have been subsequent grants. Again, as you try to set priorities in terms of what the country needs to build a national response capacity, it was clearly the consensus view of Secretary Thompson and myself that we both had a responsibility to develop a comprehensive national system to make ourselves aware as early as possible about the presence of a biological agent.

Now this, I think that dramatically improves the public health care system because regardless of whether the pathogen or that agent is brought to us by a terrorist or by Mother Nature, early detection is the best and most effective means of dealing with it.

So again, respectfully disagreeing with the notion that anything has been cannibalized, there are still quite a few dollars out there in the pipeline, some of which have not even been drawn down, to my knowledge. But the best thing we can do for the public health community generally is to develop a system where we can detect these bioagents as early as possible and then using, if necessary, the strategic national stockpile or any of the other local or State means of responding to it, that will frankly make us not only safer but I think it makes us healthier as a country. It is an investment that I think in the long run is a good investment to combat terrorism, but it is also a huge strategic investment in public health as well.

Senator LIEBERMAN. I hope to continue our work to make sure we fund all sides. As you know, I have been concerned about the coordination and consolidation of the 12 different terrorism watch lists, and I am critical of the administration for taking so long to

bring them together. I gather that they have now been consolidated. But we have heard stories, maybe fact, I ask you to respond to, that the terrorism watch list was not used, the consolidated list, during the recent Orange alert, and in that case, for instance, each flight manifest had to be checked with each terrorist watch list by the operations center at the Department of Homeland Security, which was time-consuming, labor intensive, and obviously risk prone.

I wonder if you could respond both to the status of the consolidation of the terrorism watch lists and to why it was not used during the Orange alert, if the information I received is accurate that it was not?

Secretary RIDGE. Senator, the terrorist screening center is the place under the management of the FBI but leadership from TSA where we are consolidating the 12 watch lists. The physical consolidation or technological consolidation of all watch lists in one place will continue to take several months. So right now in the Terrorist Screening Center, as we are integrating the watch list, we literally have a very labor-intensive but still very important enhancement to domestic security, a labor-intensive process where when we call upon the Terrorist Screening Center to identify a name, we have individuals in front of a screen running over the individual names. So we have access to and are using the database, but it is very labor-intensive. I believe our goal is to get the names aggregated into a single database by midsummer.

Senator LIEBERMAN. So that has not happened yet? In other words, it is not——

Secretary RIDGE. It is something that they are working on 24/7, Senator. Over the years, in order to get a particular name on a particular database, there were different thresholds of information that were required, or a different perspective depending on the agency as to whether or not the name should go on the database. Ultimately, I think we need to segregate those lists and prioritize those lists. But that integration challenge is one that we began back in December, and they are working on that piece every day.

Having said that, we have access to that information and literally have had several hundred contacts, even with State and local law enforcement agents who are beginning to use the database. Again it was labor intensive but during the most recent occasion when we had to raise the threat alert, we were able to access the Terrorist Screening Center. The operations center did it, but it is very labor intensive. We believe that by midsummer or the end of summer it should be completely integrated.

Senator LIEBERMAN. I am sorry, my time is up, but did I understand correctly that is why each flight manifest would have had to have been checked against the terrorism watch lists, because it was still being put together in one database?

Secretary RIDGE. That is why it was so cumbersome. That is why it was so time-consuming. It is not that we ignored the reality. This is information we need to have access to and use. But right now it is still a very cumbersome and time-consuming process.

Senator LIEBERMAN. Thanks, Mr. Secretary. Thanks, Madam Chairman.

Chairman COLLINS. Thank you. Senator SUNUNU.

OPENING STATEMENT OF SENATOR SUNUNU

Senator SUNUNU. Mr. Secretary, your budget includes $61 million in the Science and Technology Directorate to deal with the threat of shoulder-fired or portable anti-aircraft missiles you mentioned in your testimony. Could you provide more detail about the status of that program and how the additional money will be used?

Secretary RIDGE. Actually we have already used some of the money that Congress appropriate to us in the 2004 budget. We have had a request for proposal out. Several companies bid. We have awarded a couple contracts to companies to go through that first phase of research that they need to see if we can come up with a countermeasure, a satisfactory countermeasure, to be applied to commercial aviation. There is a misnomer that we could simply take the countermeasures that we deploy on military aircraft and just attach them to passenger aircraft. That just will not work, for a variety of reasons.

So the 2005 request is not to initiate the research. That has begun, and we anticipate that we will need those dollars to take us perhaps even to prototyping. So again, it is just a follow on to research that we have already commenced with regard to countermeasures.

Senator SUNUNU. Is the funding available through your budget, the $61 million, sufficient to keep it on track to meet current milestones?

Secretary RIDGE. We believe it is. Plus you have given us—again, the Science and Technology unit within Homeland Security has been in receipt of hundreds of millions of dollars from the Congress. And there is enough flexibility if we needed more or if we needed it sooner, we would be able to transfer dollars in. But we anticipate that that would be the cost for the next level of research, perhaps even prototyping.

Senator SUNUNU. You talked a little bit about the US–VISIT program in your testimony. Has that technology initiative resulted in greater problems or bottlenecks? Has it reduced the bottlenecks? What kind of impact has it had on the human resources that you can deploy to deal with immigration or movement at ports of entry?

Secretary RIDGE. Senator, as you are well aware, the Congress of the United States literally for years and years had requested that, not only this administration but previous administrations develop a system where we can monitor people who come across our borders and then be able to confirm their departure once their visa expired. Congress was very generous in the 2003 budget and gave us several hundred million really to affect that.

We added the requirement of a biometric identifier, feeling that while we could use just information to confirm arrivals and departures, we would be a lot better off if we were able to identify the individual who actually had the visa or the passport. To that end, we have the US–VISIT system which is basically a system based on two biometrics. One is facial recognition. The other are two finger scans. We have that deployed at 115 airports and I think 14 seaports. The consular offices around the country will have similar technology available to them all, and there is in excess of 200 of them, by October of this year so that when individuals get their visa, they will have their photograph and their finger scans taken

there. When they come to our port of entry, we will be able to confirm the identity of the visa holder, ensuring that the individual that got the visa is the one that is offering it for entry into the United States.

As you know, we are required by the Congress to come up with a system to deal with entry across the 50 largest land borders by the end of this year, and we are presently working on the technology that will enable us to affect that outcome as well.

To date we have screened over 1 million people. We have turned away in excess of 100 at the border because of information we picked up, particularly from NCIC, the criminal watch list. As we go about integrating the terrorist screening center and the other databases that we have, this information will ultimately be available and tied into the US–VISIT system as well.

Senator SUNUNU. In addition to the biometric technology, what are you doing on document verification, the ability to detect fraudulent passports, green cards or other immigration documentation?

Secretary RIDGE. First of all, the Congress has said that there is a requirement for entry by October of this year for there to be machine-readable passports prepared for our use at a port of entry. Continuing discussions with regard to the standards that should be applied to those kinds of documents are part of our conversations we are having with the European Union and elsewhere. I think one of the biggest challenges that we have, not just as a country, because the threat of terrorism and the notion that we need to ensure commercial shipping, commercial air travel, and it is a worldwide challenge that we have, is coming up with acceptable international standards based on biometrics. We are not quite there yet.

For commercial aviation, the international commercial aviation organization, their only standard is a facial scan. I think, in talking to a lot of our colleagues around the world, while that is good technology, we do need to build some redundancy into that system. So we will be working with, again, colleagues in international aviation as well as governments around the world to see if they can come up with acceptable international standards. So that work continues. We have not reached a satisfactory international standard yet as far as I am concerned.

Senator SUNUNU. Do you right now have the flexibility you need to continue to expand coverage to new ports of entry as our demographics change, as our economy changes and grows? Do you, within DHS, have the ability to bring new ports of entry into the system and to provide coverage in those expanded areas?

Secretary RIDGE. Frankly, just upgrading the personnel and equipment at existing ports of entry has been one of the primary tasks of the new Department, and I believe we have done that fairly well. When we go about talking, particularly with our colleagues in Canada and Mexico about creating new ports of entry so we can deal with the enhanced security that we want at our borders and the facilitation of commerce, that will require a significant capital investment from all of the governments. One of the things we are reviewing with our friends in Canada and Mexico, if there were to be infrastructure improvements along the border, where would they be? How much would they cost? And frankly, who would absorb the cost?

Senator SUNUNU. I am speaking specifically, and I was not clear in the question, on seaports, airports, points of cargo, and passenger entry and exit in the domestic United States that could be receiving passengers and cargo from all over the world.

Secretary RIDGE. Yes, again whether it is aviation security or commercial shipping security, the decision has been made, and I think Congress generally embraces it, that you never want to rely on a single means of security. That you need to layer in your security measures. You never want the opportunity for there to be a single point of failure.

So to that end, when it comes to commercial shipping, as you know, we began with a container security initiative. There is a targeting program based on the 24-hour requirement to provide those manifests. We board 100 percent of the high interest vessels. We have non-intrusive inspection technology both at ports abroad and in the United States. So we layer in multiple preventive measures both in aviation and in port security. I hope that answers your question.

Senator SUNUNU. It does in part. What I am getting at is the fact that reluctance or inability or lack of flexibility to distribute additional personnel can effectively prevent a seaport or an airport from growing to accept passenger transit, new immigration. There are some specific samples that I will be happy to share with your staff.

Secretary RIDGE. Thank you, Senator.

Senator SUNUNU. Thank you very much, Madam Chairman.

Chairman COLLINS. Thank you. Senator Levin.

Senator LEVIN. Thank you, Madam Chairman.

I want to start by asking you about the allocation system for homeland security grants. Two major programs here are the State Homeland Security Grant Program and the Urban Area Security Initiative when it comes to first responder grants. It strikes me that those allocations to those first responders, to the greatest degree possible, at least logically, ought to be based on vulnerabilities and threats. Every State has vulnerabilities, but there are great variations between States and localities on those vulnerabilities.

So my first question to you is, is it the administration's position that we should legislate formulas for allocating those monies that go to the States and local governments and for any State minimums? Or should that be left to the Department to adopt criteria that we would then be able to look at which would be transparent, but nonetheless would be basically departmentally determined rather than legislatively determined?

Secretary RIDGE. I believe, Senator, it would be our preference as embodied in the language for both of those grant programs, that the flexibility be given to the Department. Understanding the political reality of whether or not it can be accomplished remains to be seen, but we would certainly want to address, obviously in a transparent way, the establishment of that criteria if it was to be done internally within Homeland Security.

Senator LEVIN. So that your position is that you would rather not have them legislatively prescribed?

Secretary RIDGE. That is correct, Senator. As both of the pools of ODP dollars suggest, we do want to take into consideration pop-

ulation. But we also need to take into consideration the critical infrastructure. We need to take into consideration threats and vulnerabilities.

It is pretty difficult to come up with a mathematical formula that can deal specifically with that assessment. It is for that reason, particularly with regard to the State and local dollars through the Office for Domestic Preparedness that we have suggested for the first time in 2005, and I have said in response to Senator Collins' question that a minimum of those dollars go out to every State, but that we take a look at the State plans that have been submitted, we take advantage of the work that the States and our Department has done in identifying critical infrastructure.

Port Huron was an extraordinary example where we had a small community that had critical infrastructure around it and in it and yet I do not believe they qualified, either place, for any additional dollars. So if we had that flexibility vested in the Department I think we could address the concerns of some of those communities easier.

Senator LEVIN. Is it the administration's position that the minimum should be set by the Department or by Congress?

Secretary RIDGE. I think it would be, again, our preference that once we take a look at the state-wide plans and see what common threads and needs are there, that we would set it. But again, we welcome the notion that the Congress would work with us in order to set that criteria internally.

Senator LEVIN. I would like to go back to reverse inspections. We have been urging a system of reverse inspections where the inspection of people and cargo be done on the other side of the bridges and tunnels because it is too late once that bridge or tunnel is damaged or destroyed to inspect the cargo. We have legislated that there be at least a couple of efforts made at testing reverse inspections. What is the status of that pilot program?

Secretary RIDGE. Senator, the Smart Border Accord we have with Canada across the board has been successfully and almost completely implemented. There are still one or two areas of disagreement and reverse inspection is one of them. But with the change in administration, we have not lost our focus on that issue and our desire to convince our Canadian allies it would serve our mutual interest for both security and commerce to locate areas on either side where the inspections could take place before these vehicles move through tunnels or across bridges.

Senator LEVIN. Can you, for the record, give us the status of those pilot programs which we legislated in 2003?

Secretary RIDGE. Yes, sir.

Senator LEVIN. On the intelligence analysis coordination question and the letter which I referred to which went to four different people including yourself about the question of how do these various entities that are analyzing threats relate to each other. I guess the real question is this, we have a Department of Homeland Security, we have an FBI, we have a CIA. Internally to those we have Terrorist Threat Integration Center. In your Department we have an Information Analysis and Infrastructure Protection Directorate. We have a counterterrorism division in the FBI. And we have a CIA

counterterrorist center as well as the TTIC or Terrorist Threat Integration Center.

Who has the primary responsibility for analyzing foreign intelligence, No. 1? No. 2, is that laid out in writing? And No. 3, can we get an answer to our letter—Senator Collins' and my letter?

Secretary RIDGE. Senator, you have been very patient. You have asked me about this before.

Senator LEVIN. Uncharacteristic of me, by the way, I want you to know.

Secretary RIDGE. You have been very patient with this Secretary, and I am grateful for that because I am mindful of the date that was at the top of the letter. Having served as a former Member of Congress all I can say is I am mindful of the date, and I know it is several months later.

First of all, you ought to know that there is a coordinated response that is being prepared. The Department of Homeland Security has offered its views, and it is my understanding that response should be coming to you shortly, within the next couple of weeks.

Senator LEVIN. I just had one additional question here, but I will pass to it. Thank you.

Chairman COLLINS. Thank you. Senator Akaka.

Senator AKAKA. Thank you very much, Madam Chairman.

Mr. Secretary, I have some questions concerning the human resource system. You have requested $102.5 million for a new human resource system. As there are no final regulations in place detailing the new system, what assumptions did you make in requesting this amount? What information or precedent did you rely upon to determine that the request was sufficient to implement the system?

Secretary RIDGE. First of all, Senator, you should know that the regulations are near completion and we would anticipate the publication within the next several weeks. As you know, that kicks in a 30-day comment period and certain discussions with the men and women and their representatives from organized labor ensue after those regulations are promulgated.

The $100-plus million you refer to is a request based upon our desire to develop a performance-based pay system. It is also predicated on the notion that it is going to take some time in order to develop this system and to train managers, on the system, and how to apply it effectively. So the request for those dollars is basically to design the system, train management within the Department to utilize it appropriately and effectively, and then to begin a pilot program beginning toward the end of the year in fiscal year 2005.

One of the challenges we have, and it came up in our discussions with representatives from organized labor, of which we have had several discussions as we have developed the system, is that there is really no prototype within government. We have never been down that path before. We have been down that path in the private sector.

But it is something that the administration feels strongly about. I certainly do. I would like to have a performance-based system. But we need to design one, and we need to train people to use it effectively. There are some legitimate concerns that were raised by the representatives of the men and women that work in the Department of Homeland Security, and we thought one of the best

ways to address some of their concerns was to make sure that we implemented the approach over a period of time, not just through the initial regulation. Because it would not have been satisfactory to them, we would not have designed a satisfactory system. It is not the way to go about implementing a broad-based system. So that is the reason for the additional dollars.

Senator AKAKA. Does the $31 million earmarked for training extend beyond training managers for the implementation of a new pay-for-performance system?

Secretary RIDGE. I am sorry, I did not quite understand, Senator.

Senator AKAKA. Does the $31 million earmarked for training extend beyond training managers for the implementation of a new pay-for-performance system?

Secretary RIDGE. I think it is not just managers that have to understand the system, but I think the employees have a right to understand what is expected of them and how their performance would be recognized and rewarded. So again, primarily the training is for those who would use the system, but I think there is a broader, department-wide educational campaign that has to be undertaken once we design the system.

Senator AKAKA. Forty-two million, Mr. Secretary, has been earmarked for the design and implementation of the new human resources system and for the administration and staffing of the new labor management and appeal process. My question is, does the funding for the new human resource system include funding for the Department's recruitment and retention efforts including the use of student loan repayment?

Secretary RIDGE. I think within the Department's personnel budget there are adequate and standard resources we would use to recruit and retain people. But, Senator, it does not include any loan repayment mechanism.

Senator AKAKA. Under a pay-for-performance system, you have requested $2.5 million. How many employees will this cover? Within this amount can you provide the anticipated pay increase good performers will receive? And what information did you rely upon in making this request?

Secretary RIDGE. Senator, I believe we are looking at a small pool of employees in order to test the system for almost a year, and the additional $2.5 million was to be allocated for that purpose and, frankly, to make up for any differences that we might experience, any losses we might experience so that there will be adequate money for a pay-for-performance protocol. Again, we tried to lay this out, Senator, over the next couple of years, because it has not been done in government successfully to date. I am not sure it has been tried successfully. I know there has always been an interest in getting it done. But it is going to take us a couple years to design, train, educate, prototype, and then apply.

Senator AKAKA. I wanted to ask before my time is up, of the $300 million requested for the human capital fund to meet your pay-for-performance goals, how much do you anticipate using?

Secretary RIDGE. Senator, most of those dollars are to effect the change within the system, and it is difficult—we think we will need it all.

Senator AKAKA. Finally, information technology funding calls for $226 million. I understand that the Bureau of Immigration and Customs Enforcement has had some trouble consolidating its IT systems to perform such functions as travel, budget, and case tracking. Will this $226 million help BICE with this issue? If not, are other funding sources being made available to BICE to streamline and consolidate its IT system?

Secretary RIDGE. Senator, your question highlights one of the major technology challenges that the Department has, because as you know, some of the pieces of Homeland Security came out of legacy departments such as Commerce and Justice, and some of their information, the data that they use is integrated into their systems. So to divest this data and bring it into a consolidated system with the Department is going to take time. That applies to Immigration and Customs Enforcement. It applies to Citizenship and Immigration Services. It applies to several other units within the Department. Again, those dollars will help us, basically from a technological point of view, pull that information, pull those databases out of the legacy agencies so we can consolidate it into the Department of Homeland Security.

Senator AKAKA. Thank you. Madam Chairman, my time has expired.

Chairman COLLINS. Thank you. Senator Durbin.

Senator DURBIN. Mr. Secretary, I am a member of the Senate Intelligence Committee, and the experience we are going through now because of Dr. Kay's report is causing us to really take an assessment as to whether or not our intelligence gathering leading to the invasion of Iraq failed. The precipitate event, I suppose, was Dr. Kay's report. Fortunately, and I give you credit, the President and the administration, we have not had a sequel to September 11, 2001. God forbid that should ever occur, we will all be gathering in earnest in emergency to determine where we failed, what we could have done better.

I would like to address one or two areas that continue to trouble me. I made reference to them in my opening remarks. I do not know how we can make America safer if our computers do not speak the same language, if they are not communicating with one another, and if we disperse responsibility among different bureaucracies. I felt and I think others did as well, that your arrival and your commitment to this personally, the development of a new agency meant that a new day would dawn.

But the information that we have received suggests that the bureaucratic battles continue. Some things are very difficult for me to understand. In your last appropriation bill I asked for a report when it came to information technology by December 15. It is almost 2 months beyond that. I would commend you to note that is part of your appropriation, to give us a report on watch lists and coordination of information technology.

But let me get right down to the bottom line, if I can. It looks to me like you are losing the turf battle within this administration. I think your legislative mandate is so imminently clear, and I will read it from the bill. To access, receive, and analyze law enforcement information, intelligence information, other information of agencies of Federal Government, to integrate such information in

order to identify and assess the nature and scope of the terrorist threats to America. I thought that put you in the driver's seat.

Now let us take a look at the watch list issue. The watch list, for some reason, has been delegated to the FBI. In an answer to a question from, I believe it was Senator Lieberman, you said that you expected their effort to be fully operational by midsummer for watch list integration. When the TSC was established it was supposed to be operational by December 1.

I also want to say, not taking anything away from Bob Mueller and the fine people at the FBI, there are some questions as to whether or not this was the right place to put this watch list effort. Here we have the Inspector General's report of December of last year talking about the FBI and the FBI's efforts to improve sharing of intelligence. Listen to what the Inspector General of the Department of Justice said: "The process for disseminating intelligence was ad hoc and communicated orally from manager to staff. One CIA detailee at FBI characterized the informal process as disorganized, noting that information does not flow smoothly within the FBI, let alone externally. In the 8 months the CIA detailee had been at the FBI, the detailee had not received a single CIA intelligence report. The detailee said, 'information goes into a black hole when it comes into this building.' That is the most frightening thing I can think of, 2½ years after September 11, that we are still dealing with this. Where the President is creating by executive order agencies that compete with your legislative responsibility, agencies which frankly I think should be integrated under DHS, but instead we find in other parts of the Federal Government."

Are we making progress? It looks like you are wading through a sea of molasses here trying to get to change and reform. I believe in you. I have from the beginning and I still do. I do not like what I am seeing.

I would ask for your comment.

Secretary RIDGE. Senator, hopefully I can allay some concerns, perhaps not to your complete satisfaction but let me do my best.

First of all, the Congress has directed that our Information Analysis and Infrastructure Protection unit be supplied with adequate resources to map the threat against the vulnerability, and then the responsibility of the Department is to do something about it. What you should know is that part of the fusion operation that we do in the information analysis department and unit within Homeland Security is to take information from—we have access to the information generated by the entire intelligence community. The decision to raise the threat level over the holidays was because of the partnership and the access to information generated by the broader intelligence community, in this instance particularly by the CIA, but also other sources.

We believe that the Terrorist Threat Integration Center and the Terrorist Screening Centers add value to our effort to fuse all information from sources, whether it is horizontal across the Federal Government, whether it is vertical up from the State and locals. We are partners in the Terrorist Screening Center. We have analysts in the Terrorist Threat Integration Center. We have access to give and to make requirements on any of the information-gathering agencies in the intelligence community so that if we get a report

we are empowered by Congress to go back to that agency and ask for additional information.

So, within Homeland Security our information analysis unit is designed by the direction of Congress to fuse information from all sources, internationally, we get some information from time to time, from our own intelligence community, and from the State and locals, and that is precisely what we are doing.

Senator DURBIN. Let me ask you, I only have a few seconds left and this is such a broad question and, frankly, I do not know if you will have an opportunity to give the complete answer you would like to give, and maybe you would like to reflect on it.

As you step back, as we all step back and look at the intelligence community in America and what happened before the invasion of Iraq, where we have the director of the CIA making a speech saying in defense of his agency, we are being mischaracterized. We gave good information based on what we knew.

Now that you have to deal with intelligence, decide on alerts, decide what is truly a threat to this country, do you feel that there are fundamental weaknesses within our intelligence community which need to be addressed, beyond the partisanship here, Democrats and Republicans, that we need to address as a Nation, as you reflect on what happened prior to the invasion of Iraq?

Secretary RIDGE. Senator, I appreciate the way the question was asked, because we all have an interest in making sure that when information becomes available, regardless of the source, that is relevant to Federal action, whether it is Homeland Security, the Department of Defense, whatever, that it is actionable, that it be shared immediately so action can be taken.

I think one of the big challenges that we have as a government, and I think for that matter as a society is to understand completely how difficult information gathering and analysis is in the context of combating terrorism. We from time to time apply, I think Cold War standards of certainty to information that are not necessarily applicable to the kinds of information we can glean from multiple sources that help us combat international terrorism. There is no country, there is not necessarily a central point where we can get the information. Unlike the Cold War, we do not necessarily have satellites identifying for us troop movements, and ship movements. It is much more difficult to get human intelligence inserted into an organization like al Qaeda.

So the challenges we have, is to do exactly what you want us to do, get as much information as we can, analyze it as quickly as we possibly can. But even in that analysis there is as much art as there is science. There is probably not a day that does not go by, certainly not a week that does not go by, that we just took a look at a threat or a series of threats to the United States without considering a lot of other factors, without considering those factors you might be inclined to raise the threat level. We are very judicious about it. We will only do it when we think it is credible and corroborated. It is the notion of identifying what sources are credible, given the unique challenge of gathering intelligence in this war against global terrorism, and the unique challenge we have to corroborate that information that makes it so difficult for all of us to understand what precisely is going on.

I have enormous admiration for anyone, regardless of the administration, Republican or Democrat, who has taken upon themselves as life's work to gather and analyze information and then reach conclusions that you need to act on it in one way or the other. We are getting better at it. We are getting smarter every single day.

To your point, Senator, you have raised this question with me before with regard to the integration of technology. I would like to either come up or have Steve Cooper come up and sit down and show you what we are doing internally. I know you have questioned the 18 to 24 months. I appreciate the milestones that were set and the date certain within the calendar, but some things will get done only when—they just take time to do and I would like to come up and show you the way ahead in regards to the technology integration within the Department.

Senator DURBIN. Thank you, Mr. Secretary. Thank you, Madam Chairman.

Chairman COLLINS. Senator Pryor.

Senator PRYOR. Thank you, Madam Chairman.

Again, thank you for being here this morning, Secretary Ridge. I appreciate the task you have ahead of you. You may recall, during your confirmation process that I pretty much gave you a challenge to look at this new agency, the Department of Homeland Security, and try to make it into a model agency, try to make it one that really was the best that the Federal Government had to offer in terms of efficiency and effectiveness and teamwork. Understanding that you inherited a lot of people from other agencies and other existing institutions, and also you brought in—some are absolutely a new creation.

So I would like to hear your comments on how you think the agency is running, and how it is doing in this challenge that I have laid out, and other Members of the Committee have laid out, to be a model Federal Government agency. I would just like to hear your comments, and then if you could even grade yourself on the job you have done up to this point.

Secretary RIDGE. If you give anybody the opportunity to make up the test, take the test, grade the test, I would tell you it is easy. It is easier. If it only were that easy.

Senator one of the most significant challenges with this whole enterprise is that basically with the direction, and support of Congress, I might add, we are dealing with an organization that has within it a couple of startups, a few mergers, and an acquisition or two as well as a divestiture, to put it in private sector terms. So we have got a lot of things going on. One of the biggest challenges has been to maintain the focus day to day at the borders, at the airports, with the ports, to maintain that operational effectiveness and actually improve it at the same time we are integrating personnel systems, information systems, fiscal systems, procurement systems.

I would tell you that my sense is that we have accelerated that process rather dramatically the past 3 or 4 months. The acceleration initially was slow simply because putting together a leadership team requiring background checks, Senate confirmation took a while, and very appropriately; it should. But now that we have got the leadership team in place, the vision is clear, the mission is

clear, our performance goals have been articulated and that from day one on March 1 we started doing things differently at our ports of entry.

Where you had at one time three agencies, three different Federal employees wearing three different uniforms and three different chains of command, immediately we consolidated that so they were all working with one chain of command and in the future—they have now and in the future are going to be cross-trained to do all of those tasks. So then we have more people to do more things at ports of entry which means when we have a surge need, that there are more people coming into the airport, people coming into the border, and we can put more people in order to meet the surge.

You will see innovations like this throughout. The US–VISIT system is something that Congress had mandated we get done. No one thought we could get it done, but we were able to achieve it. Working on the human resource management system, it is a real challenge. Congress gave us the opportunity to do it, but we want to do it right, so we spent a lot of time—we have had several meetings around the country talking to employees. We certainly talked to their leadership. That rule will be promulgated probably by the end of this month.

You have given us the resources to make dramatic changes at the airports. We have leaned forward to begin the process of protecting America and address our concern about port security in ports around the world. As we speak today, we have inspectors at Shanghai and Hong Kong and Rotterdam and elsewhere who begin that targeting process, who begin inspecting the cargo. Sometimes it is a physical inspection. Sometimes it is where they open it. Other times it is with non-intrusive technology. So while we try to make operational improvements, we have also tried to pull our resources together to begin the process of integrating all the enabling management functions.

You will get a more complete report card on or about March 1. I think we have made great progress but I will be the first one to admit in terms of operational efficiency we have done well. We are going to do better. In terms of integrating some of the enabling management personnel that we have and functions that we have, we have done well. We are going to do better. But I think the pace has accelerated considerably the last 3 or 4 months.

You notice I avoid giving myself a grade. It would be too self-serving.

Senator PRYOR. I did notice that.

Secretary RIDGE. I wish I could have done that in college.

Senator PRYOR. I am not going to press on that. I must tell you that my background as being Arkansas's Attorney General I am very connected to the law enforcement community in my State and when I talk to folks in the law enforcement community, mayors, people, firefighters, etc., one complaint I still hear is the slowness of money coming out of the Federal Government down to the local level to first responders. In fact today there is a story on *Fox News* online about that and they quote a number of people that are out and around the country doing different things, and that is still a complaint. So I have heard that in my offices. It sounds like nation-

ally people are hearing that, and I would like to hear your response on that.

Secretary RIDGE. We are hearing it as well, Senator. First of all, let me assure you that the dollars that you appropriated to the Department in 2002, 2003, and 2004, particularly the 2002 and 2003 dollars, they are ready to be drawn down. We have done our job. You told us to get it ready for distribution within 45 days and we were ready.

Having said that, looking at our partners, and they are our partners at the State and local level, we know that depending on the State there are different reasons for the delay. We are going to take it upon ourselves with our partners to try to break the logjam and then come up with a standard means of distribution so that neither you nor your colleagues on the Committee or other Members of Congress, and more importantly, the first responders will ever say again it is taking too long to get those dollars to us.

Clearly they are right. We have $8 billion to $9 billion to be distributed. Some have not been distributed from 2002 yet. We still have almost half from 2003, if not more, let alone the 2004 dollars. So there is a problem there. We are ready to make the distribution.

So we are going to go back and take a look at the States that have done a good job of distributing the funds and see what practices they employ, and then sit down—frankly, I am going to sit down with the governors when they come to town in a couple weeks to talk about the distribution problem because we all want those dollars, once appropriated, to get out to where the governors and the mayors and the first responders have prioritized their needs. The sooner, the better.

Senator PRYOR. Madam Chairman, let me ask one follow-up question on that, if I may. I have been looking at the President's budget and I know that you have sat in that chair right there over the last 12 months and you have reiterated time and again the importance of having local law enforcement on board. You just mentioned again it is teamwork, you are partners, etc. But how can we expect preparedness at the local level when in the President's budget we are cutting the dollars available to local law enforcement agencies and first responders by about $800 million?

Secretary RIDGE. I think, first of all, I want to try to put again into context, every year we are going to make an assessment as to what the priorities of the Department of Homeland Security are. I believe the level of funding requested by the President this year is fairly close to the level of funding the President requested last year and then Congress added several hundred million dollars to that request. You will note that we have maintained the same level of funding, knowing full well that if we get this level as requested that there would have been nearly $15 billion out to the States and to the locals since 2001, and most of that in the past 3 years. Our focus, as we maintain the same level of funding we requested last year as this year is to not only worry about inputs but outcomes.

We take a look at 2005 as being a critical year as we take a look at the homeland security strategies submitted by the States, taking a look at their needs so we can better distribute the dollars. I think Congress will hold the Department accountable for where the dollars have gone. We accept that responsibility. We maintain the

same strong level of funding, $3.5 billion, but this year for purposes of the budget a little more money for the Coast Guard, more money for biosurveillance, more money for the human resource plan, were priorities that were funded. And again, maintaining a $3.5 billion fund for first responders was considered appropriate under the fiscal and security circumstances with which we operate.

Senator PRYOR. Thank you, Madam Chairman.

Chairman COLLINS. Thank you.

Mr. Secretary, we are going to do a very brief final round of questions of only 3 minutes each in the attempt to get you out of here as near to 12 noon as possible. We appreciate your time this morning.

In my remaining few minutes I want to bring up two problems that my home State has experienced. I bring them up not only to bring them to your personal attention in the hope of securing a commitment that your staff will work with us to resolve them, but also because I believe they illustrate some of the broader issues that the Department is confronting as it seeks to strengthen our homeland security.

The first involves a community in far northern Maine, in northwestern Maine, that has a very difficult situation because the houses are on the American side of the border and all the services that this community uses are on the Canadian side of the border. So to go to church, to avail themselves of medical care, and to go to the grocery store, these American citizens need to cross over to the Canadian side.

Prior to the tightening of security, the Department had a program called the Form One program that allowed these citizens to get certified by our government, if you will, and to be able to cross at will. So to go to Catholic mass on Sundays, for example, was a very easy undertaking.

Now, however, there is a gate at that border which is unmanned on Sundays, and the result is that these citizens are essentially locked in on the American side of the border. They would have to travel over 100 miles through woods roads in order to cross at a different border crossing. This creates a real hardship for their lives, and it has also led to some of the citizens in frustration crossing illegally and then fines being imposed on them. It is just a very difficult situation given that all the services are on the Canadian side.

I would note, the Canadians still have a system that allows these citizens to enter Canada without any problem whatsoever. The problem is they cannot get back. They cannot cross back over to their homes on the American side.

The Department in response to my request did institute some limited Saturday hours which were helpful, but that has not solved the problem on Sundays or evenings, and it is a real problem. There are not a lot of people involved but it has completely changed their lives, and it illustrates the problems between free flow of people and commerce who are not going to do our country any harm versus the need to have tighter control over our borders.

The second incident involves a recent sweep by Immigration and Border Patrol officials in Portland, Maine. This sweep resulted in 10 arrests, and obviously we want the Department to vigorously

enforce our immigration laws. There were some people who were there illegally and there were those who were there on expired visas. But we also had many serious complaints from community leaders that the way in which this sweep was conducted created a great deal of fear among immigrants who are here legally. The agents went to a homeless shelter, they targeted Latino, Asian, and African restaurants, which then experienced a dramatic drop in business throughout this period.

It just seems to me that there has to be a better way for the Department to pursue its very important responsibilities and to make sure that people are not here illegally. I do feel strongly about that. But to work more with the community involved to make sure that these sweeps are conducted in a way that is respectful of people and do not target small businesses in a way that ends up hurting their business.

So I would ask that you work with me and the Department work with me on those two issues. Neither of them are easy issues and I think both of them illustrate the challenges and the problems that we face in this new September 11 world.

Secretary RIDGE. Senator, it would be a pleasure to work with you on both of those. They are illustrative of the challenges, not just the Department or your particular community face, but the entire country, and that is the balance between aggressive enforcement of the law, be it for law enforcement purposes or counter-terrorism, anti-terrorism purposes and a dramatic change in how we have historically done business. I suspect that community that has been affected adversely by the gate across what had heretofore been just a normal path of entry and exit is probably mirrored across the entire northern border. So I think, obviously, we would be pleased to work with you on that. It is that balance between security and convenience and commerce that sometimes needs to be applied on ad hoc cases, one at a time. So obviously we will be pleased to work with you on that.

I would say, hopefully, if men, women, and children are in this country legally they have nothing to fear and should not fear. We need to maintain ourselves as that open, welcoming country that we have been for 200 years. How they conducted business on that particular day or days I am not familiar, whether or not notice was given to the local communities, whether or not they engaged local law enforcement to assist them, I cannot answer that question. But I suspect if we put some of my folks down with yours we will be able to get to the answers.

We do not want to discourage the Border Patrol from doing their job. We also want to encourage them to do it in a way that is consistent with the standards of service of the Border Patrol and that is respecting the rights of individuals, be they legal or illegal, and the rights of the community. So again, it is obviously a situation that you and I have to explore and if there is a need for a remedy or a change in approach, then I would be pleased to discuss it with you.

Chairman COLLINS. Thank you very much, Mr. Secretary. Senator Lieberman.

Senator LIEBERMAN. Thank you, Madam Chairman.

Mr. Secretary, this last round I would like to give you three questions and you can answer them to the extent that time allows, although I hope they lend themselves to rather brief answers. The first is on the question of interoperability. As we know, on September 11 there is some substantial reason to believe that some of those first responders we lost at the Trade Center certainly were lost because of a failure to communicate with their colleagues, brothers and sisters in law enforcement.

This capacity to communicate with one another is lagging in most parts of the country today. I saw one cost estimate that said it could cost $18 billion to create real interoperable communications. The President's budget this year appears to cut the minimal funding that was targeted to interoperability in the past budgets through FEMA and the Department of Justice. So my question is, what role the administration sees in making interoperability a reality among local law enforcement?

Second, we talked before about the terrorism watch list. My initial thought—and I am not alone in this dream here—was that we would eventually have a coordinated watch list that would, using your terms, not only be horizontal but vertical and that any local police officer stopping somebody for a traffic violation, just as they punch into the crime information system now, would be able to punch in similarly to a terrorism watch list, and might apprehend somebody who was on that list. I wanted to ask you whether you share that goal and how we are doing in achieving it.

Then the final, on the TSA—again, we cannot do everything right away but with the enemies that we have who are going to strike at our vulnerabilities, I think one of our roles here is to be persistent in pressuring each other to limit and close those vulnerabilities. In the TSA budget, which now looks to be over $5 billion, I find only $24 million assigned to what I would call non-aviation modes like rail, bus, trucks, etc. What is the priority that you can place or you think the budget should place on the non-aviation transportation modes which themselves, unfortunately, might be vulnerable targets for terrorists?

Secretary RIDGE. Madam Chairman, if I could have a few extra minutes to respond, as I think I would like to answer the Senator's questions.

Chairman COLLINS. Absolutely.

Secretary RIDGE. First of all, Senator, the whole question of interoperability, communications, is very much at the heart of equipping our first responders to do the best job they possibly can at the time of an incident. Their primary job is to save lives, and until we come up with an interoperable communication system, we will not be able to maximize their personal effort.

To that end, SAFECOM, that acronym has been used in a couple different places, but safe communications, there are three pilot projects, there are several pilot projects out right now and that is one of the areas that the science and technology unit is examining for the purpose of determining the standards we need in order to create such a system.

I would tell you that as an eligible drawdown on some of these dollars from the Office for Domestic Preparedness there is technology on the market that basically can be used to secure basic in-

formation from different sources on different frequencies, translate it, and then ship it out. That is only a temporary measure.

So first, we have pilots working. Second, there is some technology on the market that can assist with this. It is not the final answer. And third, the whole notion of standards is part of the Science and Technology's mission.

With regard to vertical information sharing, the notion that once we have the watch list integrated into one database, and we will be there, and I believe, by the end of the summer, rather than individuals sitting in front of screens looking at their individual watch lists, the notion that it should be shared with the State and locals is one that we all embrace.

Senator you should know that most of the inquiries to date to the terrorist screening center have been from State and local law enforcement. Again, it just shows you what a powerful tool information is when you get it in the hands of people who can take action with it. So again, we are going to do better at the integration and we are looking for ways within the Department of Homeland Security on how we can better share that information via the Internet and elsewhere with State and locals under other circumstances as well. So that process is moving along rather swiftly and I think effectively.

Senator LIEBERMAN. Can I stop you? I apologize. In other words, what you said, the No. 1 customer, if you will, or the source of questions to the terrorism watch list now, are from State and local law enforcement?

Secretary RIDGE. Not the No. 1, but the first couple inquiries we had within——

Senator LIEBERMAN. They picked somebody up and they wondered whether there was something to worry about?

Secretary RIDGE. Correct. Now ultimately that integrated database will be connected into the airports, the TSA, and the ports of entry. But that is precisely what happened. They are anxious to help, Senator. You know that.

Senator LIEBERMAN. They sure are.

Secretary RIDGE. These State and local folks, 650,000 strong, they want to help. And one of the best things we can do to enlist their support is to get them the information they can act on.

Third, Congress has provided, you are right, the bulk of the funding for TSA as it relates to aviation security. But separate and apart from that, when it comes to other forms of transportation, shipping, you have got the Coast Guard, and as we take a look at rail and trucking, etc., you have given us quite a few dollars in the infrastructure protection budget to take a look at technologies that can apply to improving security. It is part of our responsibility as well to work with the agencies that also oversee these other modes of transportation, the Federal Highway Administration and the like, to work on improving safety and adding more security to those venues as well.

Senator LIEBERMAN. Thanks, Mr. Secretary. Obviously we have come a long way and we have got a long way to go and we are going to get there quickest if we go there together, so I look forward to it. Thanks, Madam Chairman.

Secretary RIDGE. Thank you, Senator.

Chairman COLLINS. Thank you. Senator Akaka.

Senator AKAKA. Thank you very much, Madam Chairman.

I have three quick questions. One that follows up on the Chairman's concern on immigration. I understand that BICE is reorganizing the special agent in charge of field office structure. My question is, how does the budget request cover this reorganization?

My second question has to do with cuts in science and technology in the university and fellowship programs within Science and Technology Directorate, a cut of $38.8 million. My question is, why were these programs cut? Because I feel such programs certainly develops the innovative and skilled technical staff that we need.

Finally, on geospatial information databases. I have long had an interest in using geospatial information to enhance our response to disasters. A comprehensive and layered national defense database of geospatial information could be an essential element in developing a comprehensive response to any disaster. Indeed, such information was useful in response to the September 11 disaster in New York. My question is, does the Department have a strategy for acquiring such a capability? If so, what is the timeframe for its development?

Secretary RIDGE. First of all, Senator, with regard to seeking additional dollars to reorganize the Bureau of Immigration and Customs Enforcement, we think the Congress has been generous in supporting the basic function of BICE. You gave us an increase this year and as far as we are concerned, it is our responsibility to reorganize it, to make it as efficient as possible and we should not be knocking on your door to get additional money to do it. You have already been pretty generous.

Second, the science and technology question that you asked, I did not hear, Senator, the specific reduction in funding that you were concerned about. I know it was in S&T but I did not quite pick that up. Could you kindly repeat that?

Senator AKAKA. Yes. The budget proposes a cut of $38.8 million in the university and fellowship programs within the Science and Technology Directorate. My question, why were these programs cut and what do you think about whether it affects the Department's ability to develop and maintain the most innovative and skilled technical staff possible?

Secretary RIDGE. Senator, as you know we have begun both a program to identify and work with centers of excellence—those are academic institutions around the country—and the scholars and fellows program. Again, as we took a look internally as to what we thought our priorities should be for fiscal year 2005 we thought we could maintain the existing program with regard to scholars and fellows and maintain the existing number of centers for academic excellence, but for the fiscal year 2005 there were other higher priorities and chose to fund those. But make no mistake about it, over the long term, scholars and fellows for the science and technology unit will continue to be a significant priority. It is just not the highest priority this year.

In the academic centers of excellence which to date, Senator, have ended up being grants given to universities that consolidate their applications, the first one was given out West but actually involved five universities all around the country. So again, in 2005,

set priorities, we will maintain the existing fellows and scholars program. We will maintain—I think we are going to have four to six academic centers of excellence. But the priorities for 2005 said, maintain and grow them later.

Senator AKAKA. My final question was on geospatial information database and asking for a timeframe for its development.

Secretary RIDGE. Senator, I know that in discussing the geospatial component of both our operations center and talking with people in FEMA about it and others that there is significant interest within the Department. I cannot speak specifically whether or not it has been reduced to a strategy, and I would welcome the opportunity to address that by virtue of a letter to you here in the next week or so.

Senator AKAKA. Thank you very much, Madam Chairman.

Chairman COLLINS. Thank you, Senator.

Mr. Secretary, thank you not only for appearing this morning but for the outstanding leadership that you have given the Department during its first year in operation. We very much appreciate your leadership and your dedication to public service.

Secretary RIDGE. Thank you, Senator. Thank you very much.

Chairman COLLINS. This hearing record will remain open for 15 days for the submission of additional materials. I want to thank my staff and the Minority staff for their hard work in putting together this hearing which is now adjourned. Thank you.

[Whereupon, at 12:10 p.m., the Committee was adjourned.]

APPENDIX

Statement of Secretary Tom Ridge
before the United States Senate
Committee on Governmental Affairs

February 9, 2004

Introduction:

Chairman Collins, Senator Lieberman and Members of the Committee:

I am honored and pleased to appear before the Committee to present President Bush's FY 2005 budget for the Department of Homeland Security. Before beginning to outline our FY 2005 budget request, I want to thank you for the strong support you showed for the Department in the FY 2004 budget and for the fact that that appropriation was passed in time for it to be signed by the President on October 1, 2003 – the first day of the fiscal year.

The $40.2 billion request represents a ten percent increase in resources available to the Department over the comparable FY 2004 budget and reflects the Administration's strong and continued commitment to the security of our homeland. The fiscal year 2005 budget is a $3.6 billion increase over fiscal year 2004, and it includes increased funding for new and expanded programs in border and port security, transportation security, immigration enforcement and services, biodefense, incident preparedness and response, and the implementation of a new human resources system that will reward outstanding performance. The budget also continues our momentum toward integrating intelligence, operations and systems in a way that increases our nation's security.

The Department of Homeland Security has made great organizational strides during the first year of operations. Nearly 180,000 employees and a budget of $31.2 billion were brought under DHS less than a year ago. The Department established a headquarters operation and successfully began operations on March 1, 2003 – bringing together the legacy agencies and programs that now make up DHS. Customs, border and immigration activities have been reformulated into new agencies that will increase the effectiveness of our dedicated employees. DHS continues to create new ways to share information and intelligence within the Department and between levels of governments, and horizontally across agencies and jurisdictions. Already, over 350 different management processes have been consolidated to 130, and DHS has begun consolidating 2,500 support contracts into roughly 600.

While DHS invested considerable time to make the many organizational improvements that will improve our effectiveness, much was also accomplished programmatically. The fiscal year 2003 Performance and Accountability Report provides a comprehensive discussion of our accomplishments of the past year. We believe that in the twelve months since the creation of the Department, we have made substantial progress. Through the hard work of our dedicated and talented employees, America is more secure and better prepared than we were one year ago.

We have achieved many results since our creation, including:

- improving the collection, analysis and sharing of critical intelligence with key federal, state and local entities;
- allocating or awarding over $8 billion to state and local first responders to help them prevent and prepare to respond to acts of terrorism and other potential disasters;
- strengthening border security through the "One face at the border" initiative, which will cross-train officers to perform three formerly separate inspections—immigration, customs and agriculture. This will allow us to target our resources toward higher risk travelers;
- instituting innovative new systems like US-VISIT to identify and track foreign visitors and students and to screen for possible terrorist or criminal involvement;
- safeguarding air travel from the terrorist threat by hardening cockpit doors, instituting 100 percent checked baggage screening; and training more than 50,000 federal passenger and baggage screeners;
- increasing safeguards on maritime transportation and port infrastructure;
- expanding research and development in the defense of our homeland, through the creation of programs such as the Homeland Security Advanced Research Projects Agency (HSARPA) which has already engaged hundreds of private companies and universities in developing new cutting-edge technologies;
- launching an ambitious, collaborative effort involving input from employees at all levels, unions, academia, and outside experts to design a modern human resources system that is mission-centered, fair, effective and flexible;
- initiating a five-year budget and planning process and commencing the development of an integrated business and financial management system (Project eMerge^2) to consolidate the 50 different budget execution systems, 43 different general ledgers, and 30 different procurement systems inherited by DHS; and
- successfully transferring more than $50 billion in assets, $36 billion in liabilities and more than 180,000 employees to the Department.

FY 2005 Budget Request

The Fiscal Year 2005 budget for the Department of Homeland Security builds upon the significant investments to date to our safeguard against terrorism, while also sustaining the many important departmental activities not directly related to our fight against terrorism. The President's budget clearly demonstrates the continuing priority placed on the Department of Homeland Security in providing total resources for FY 2005 of $40.2 billion. This is an increase of 10% above the comparable FY 2004 resource level, $9 billion (29 percent) over the 2003 level and $20.4 billion (103 percent) over the 2001 level.

Strengthening Border and Port Security

Securing our border and transportation systems continues to be an enormous challenge. Ports-of-entry into the United States stretch across 7,500 miles of land border between the United States and Mexico and Canada, 95,000 miles of shoreline and navigable rivers, and an exclusive economic zone of 3.4 million square miles. Each year more than 500 million people, 130 million motor vehicles, 2.5 million railcars, and 5.7 million cargo containers must be processed at the border. Conditions and venues vary considerably, from air and sea ports-of-entry in metropolitan New York City with dozens of employees to a two-person land entry point in North Dakota.

During FY 2005, we will continue to strengthen our border and port security. Our budget seeks over $400 million in new funding to maintain and enhance border and port security activities, including the expansion of pre-screening cargo containers in high-risk areas and the detection of individuals attempting to illegally enter the United States. Our budget also includes an 8 percent increase for the Coast Guard to upgrade port security efforts, implement the Maritime Transportation Security Act, and enhance other activities.

Specifically, our budget includes an increase of $25 million for U.S. Customs and Border Protection's Container Security Initiative (CSI) which focuses on pre-screening cargo before it reaches our shores. We are also seeking an increase of $15.2 million for Customs Trade Partnership Against Terrorism (C-TPAT). C-TPAT focuses on partnerships all along the entire supply chain, from the factory floor, to foreign vendors, to land borders and seaports. To date, nearly 3,000 importers, 600 carriers, and 1,000 brokers and freight forwarders are participating in C-TPAT, surpassing the Department's original goal of participation of the top 1,000 importers. In order to further protect the homeland against radiological threats, the budget seeks $50 million for next generation radiation detection monitors.

As well as continuing development for secure trade programs, the President's budget also seeks an increase of $20.6 million to support improvements for the National Targeting Center and multiple targeting systems that focus on people and/or goods. These systems use information from diverse sources to provide automated risk assessments for arriving international air passengers, shipments of goods to our country, and land border passenger traffic.

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program's goals are to enhance the security of our citizens and our visitors; facilitate legitimate travel and trade across our borders; ensure the integrity of our immigration system; and respect the privacy of our welcomed visitors. US-VISIT represents a major milestone in our efforts to reform our borders. DHS deployed the first increment of US-VISIT on time, on budget, and has met the mandates established by Congress as well as including biometrics ahead of schedule. The budget seeks a total of $340 million in FY 2005, an increase of $12 million over the FY 2004 level. Through FY 2005, over $1 billion will be used to support this initiative.

Our budget also seeks an increase of $64.2 million to enhance land-based detection and monitoring of movement between the ports, and $10 million to plan, procure, deploy and operate unmanned aerial vehicles. In addition, the budget request for U.S. Immigration and Customs Enforcement (ICE) includes an increase of $28 million to increase the flight hours of P-3 aircraft. The P-3 has already proven itself to be a key asset in the battle against terrorism as demonstrated in the days immediately following the September 11, 2001 attacks when P-3s flew airspace security missions over Atlanta and Miami.

The Coast Guard funding increase includes over $100 million to implement the Maritime Transportation Security Act, to support the Coast Guard's ability to develop, review and approve vessel and port security plans, ensure that foreign vessels meet security standards, improve underwater detection capabilities, and increase intelligence capacity. The budget also maintains the Coast Guard's ongoing Integrated Deepwater System initiative, funding the program at $678 million, an increase of $10 million over the FY 2004 funding level.

Enhancing Biodefense

The President's FY 2005 budget reflects $2.5 billion for Project BioShield that will be available in FY 2005 to encourage the development and pre-purchase of necessary medical countermeasures against weapons of mass destruction. Project BioShield allows the Federal Government to pre-purchase critically needed vaccines and medications for biodefense as soon as experts agree that they are safe and effective enough to be added to the Strategic National Stockpile. The Administration is moving forward in purchasing the most important countermeasures and high on the list are next-generation vaccines for both smallpox and anthrax.

The Department's efforts to improve biosurveillance will involve the Information Analysis and Infrastructure Protection (IAIP) and Science and Technology (S&T) directorates. In S&T, the budget requests $65 million increase to enhance current environmental monitoring activities, bringing the total FY 2005 investment in this area to $118 million. One key component of this initiative will be an expansion and deployment of the next generation of technologies related to the BioWatch Program, a biosurveillance warning system. In IAIP, $11 million increase is included to integrate, in real-time, biosurveillance data collected from sensors throughout the country and fuse this data with information from health and agricultural surveillance and other terrorist-threat information from the law enforcement and intelligence communities.

The National Disaster Medical System (NDMS) is responsible for managing and coordinating the Federal medical response to major emergencies and federally declared disasters. For 2005, FEMA's budget includes $20 million for planning and exercises associated with medical surge capabilities. In addition, the budget transfers funding ($400 million) for the Strategic National Stockpile to the Department of Health and Human Services to better align the program with that agency's medical expertise.

Improving Aviation Security

We have made great strides to improve the safety of the aviation system from acts of terrorism. For example, we have made significant investments in baggage screening technology – over $2 billion to purchase and install Explosive Detection System machines (EDS) and Explosive Trace Detection machines (ETD) to the nation's airports from FY 2003 to FY 2005; hardened cockpit doors; deployed 45,000 federal passenger and baggage screeners at the Nation's airports; and trained pilots to be Federal Flight Deck Officers. The President's FY 2005 budget seeks to enhance our efforts in this regard and would provide an increase of $892 million, a 20 percent increase over the comparable FY 2004 level, for the Transportation Security Administration (TSA). Additional funding for TSA supports aviation security, including efforts to maintain and improve screener performance through the deployment of technology.

The Department implemented a substantially improved air cargo security and screening program last year, and the President's budget sustains funding to continue program deployment and screening technology research. In addition, the FY 2005 budget seeks a total of $61 million to accelerate development of more effective technologies to counter the threat of portable anti-aircraft missiles.

Enhancing Immigration Security and Enforcement

Comprehensive immigration security and enforcement extends beyond efforts at and between the ports-of-entry into the United States. It extends overseas, to keep unwelcome persons from reaching our ports, and to removing persons now illegally residing in the United States. The Administration is committed to stronger workplace enforcement in support of the President's temporary worker proposal announced January 7, 2004.

The requested increases include $186 million for U.S. Immigration and Customs Enforcement (ICE) - whose appropriated budget overall increases by about 10 percent - to fund improvements in immigration enforcement both domestically and overseas, including more than doubling of current worksite enforcement efforts and approximately $100 million increase for the detention and removal of illegal aliens. Detention and Removal of illegal aliens present in the United States is critical to the enforcement of our immigration laws and the requested funding will expand ongoing fugitive apprehension efforts, the removal from the United States of jailed illegal aliens, and additional detention and removal capacity.

Our proposal for ICE also includes an increase $78 million for immigration enforcement. As part of the President's proposed new temporary worker program to match willing foreign

workers with willing U.S. employers, enforcement of immigration laws against companies that break the law and hire illegal workers will increase. The FY 2005 President's Budget includes an additional $23 million for enhanced worksite enforcement. This more than doubles existing funds devoted to worksite enforcement and allows ICE to hire more Special Agents devoted to this effort. With these resources, ICE will be able to facilitate the implementation of the President's temporary worker program initiative by establishing a traditional worksite enforcement program that offers credible deterrence to the hiring of unauthorized workers. Without such a deterrent, employers will have no incentive to maintain a legal workforce.

Our budget also seeks $14 million to support our international enforcement efforts related to immigration, including enabling ICE to provide visa security by working cooperatively with U.S. consular offices to review visa applications.

We are a welcoming nation, and the hard work and strength of our immigrants have made our Nation prosperous. Within the Department, the U.S. Citizenship and Immigration Service (CIS) has improved the administration of immigration benefits to the more than seven million annual applicants. For FY 2005, the President's budget seeks an additional $60 million, for a total of $140 million, to achieve a six-month processing for all immigration applications by 2006, while maintaining security.

Increasing Preparedness and Response Capability

Though the primary mission is to protect the Nation from terrorism, the Department's responsibilities are diverse. The ships that interdict threats to our homeland are also used to help mariners when they are in distress and protect our marine resources from polluters and illegal fishing. While we must be prepared to respond to terrorist attacks, we are more often called upon to respond to natural disasters

To support the Department's efforts to respond, the President's Budget includes an increase of $10 million, for a total of $35 million in FY 2005, for the Homeland Security Operations Center (HSOC). Pursuant to the Initial National Response Plan, the HSOC integrates and provides overall steady state threat monitoring and situational awareness and domestic incident management on a 24/7 basis. The HSOC maintains and provides situational awareness on homeland security matters for the Secretary of Homeland Security, the White House Homeland Security Council and the federal community. In addition, the HSOC provides the Department's critical interface to all federal, state, local & private sector entities to deter, detect, respond and recover from threats and incidents.

The National Incident Management System (NIMS) is designed to ensure that all levels of government work more efficiently and effectively together to prepare for, respond to, and recover from domestic emergencies and disasters, regardless of cause. For FY 2005, the Department requests $7 million to ensure that the major NIMS concepts involving incident command, coordination, communication, information management, resource management, etc., are incorporated into and reflected in FEMA's national disaster operational capability. This

funding will provide for plan development, training, exercises and resource typing at the Federal, State, and local levels

Supporting State and Local First Responders

The Department has initiated consolidation of the two principal offices responsible for administering the grants awarding process for emergency responders and State/local coordination, the Office of State and Local Government Coordination and the Office of Domestic Preparedness. This consolidation provides an opportunity to tie all DHS terrorism preparedness programs together into a cohesive overall national preparedness program designed to support implementation of State Homeland Security Strategies.

The FY 2005 budget continues to support the Nation's first responders and seeks a total of $3.6 billion to support first-responder terrorism preparedness grants with better targeting to high-threat areas facing the greatest risk and vulnerability. For FY 2005, funding for the Urban Area Security Initiative (UASI) doubles from $727 million to $1.45 billion. Since March 1, 2003, DHS awarded or allotted over $8 billion to support state and local preparedness. Between FY 2001 and the FY 2005 budget request, over $14 billion in assistance will be made available for programs now under DHS. Our request for FY 2005 is slightly higher than funding sought for these programs in FY 2004.

Investing in Human Capital and Building Departmental Infrastructure

Our employees are our single greatest asset and we are committed to investing in the development and motivation of our workforce. To support our efforts in creating a model personnel system, the President's FY 2005 budget seeks $133.5 million for the implementation of a new DHS human resources system that is mission-centered, fair, and flexible by rewarding top performers. The FY 2005 budget specifically provides additional resources that will be used for training supervisory personnel to administer a performance-based pay system and to create the information technology framework for the new system. Our new system will ensure that DHS can manage and deploy its resources to best address homeland security threats and support information technology tools for workforce management.

We also seek additional funds to invest in the Department's core infrastructure. Our budget request seeks a total of $56 million, an increase of $17 million to support a new resource management system. This funding will support the design, development, and implementation for a single Department-wide financial management system. It will provide decision-makers with critical business information, e.g., budget, accounting, procurement, grants, assets, travel, in near "real-time" and eliminate stovepipes within existing systems and processes.

An increase of $45.1 million is also sought to continue expanding the DHS presence at the Nebraska Avenue Complex (NAC). These resources will enable DHS to perform tenant improvements to the facility and relocate U.S. Navy operations, pursuant to congressional authorization, from the NAC to leased facilities.

Conclusion:

We have a dedicated and skilled team in DHS who understand that what they are doing is important. We have the support of our partners in government and the public and private sectors. I thank the Congress for its support, which has been critical to bringing us to this point.

Our homeland is safer than it was a year ago, but we live in dangerous times and cannot count on times to change. That is why the Department of Homeland Security was created, and why we are moving forward. I am grateful to be here today to talk about the work we are doing to make America a safer home for us, for our children and generations to come.

Thank you for inviting me to appear before me today, and I look forward to answering your questions.

Post-Hearing Questions for the Record
Submitted to the Honorable Tom Ridge
From Senator John Sununu

Senate Committee on Governmental Affairs Hearing Entitled: The Department of Homeland Security's Budget Submission for Fiscal Year 2005

February 9, 2004

Note: *The responses to the Questions for the Record (QFRs) were drafted to be accurate as of the date of the hearing, February 9, 2004, in part due to the subject of the hearing: the President's budget request for DHS for FY2005. As such, EO 13356, the Intel Reform Act, and the NCTC did not exist, and are, therefore, not addressed in the responses.*

Mr. Secretary, I want to follow up on my last line of questioning at this morning's hearing. At that time, I asked you if the Department can and will be able to meet the needs of growing airports and/or seaports that currently do not require DHS staffing, or require minimal staffing by screeners and Customs inspectors. I asked this question in general terms but my concern relates specifically to a situation at the Pease International Tradeport (KPSM) in Portsmouth/Newington, NH.

In 1998, a new commercial air terminal opened at Pease, a former Air Force base. This facility has the ability to accommodate international flights and, when it opened met all requirements to process large passenger jets of international origin. Currently, flights chartered by the Department of Defense to bring soldiers home from operations in Afghanistan and Iraq, would like to land at Pease to refuel and have passengers cleared through Customs before arriving at their final destinations here in the U.S. There are no Customs inspectors stationed at Pease, but inspectors can be sent from the Port of Portsmouth as well as Boston and Portland, ME. However, Customs is unwilling to deviate from the status quo and so far the Bureau has refused to accommodate this request for new service, citing funding and manpower shortages.

My office has been working with Senator Gregg's office, the Pease Development Authority, and Customs for months to try to resolve this situation. There are post-9/11 modifications that need to be made to the facility to accommodate international flights, but Customs will not tell airport officials what modifications are needed for another two or more months. At the current pace, it could be many months--even a year or more--before these and similar flights could be allowed to land at Pease. Meanwhile, these Department of Defense charter flights and other business are being turned away because Customs will not provide service.

If DHS is unable to increase its level of service to meet the growing demands of air and seaports like Pease, the continued economic growth of the New Hampshire seacoast and other regions will be suppressed. You and the men and women of your Department operate under the mission of providing homeland security without impeding the free flow of commerce. Do you feel this budget request, if approved by Congress, provides the Department with the needed flexibility to respond to growth at Pease and other facilities to meet their needs for services provided by DHS?

Answer: The Pease International Tradeport issue is currently under review by U.S. Customs and Border Protection (CBP), Office of Field Operations (OFO). OFO has conducted a study of the facility to determine what additional security modifications will need to be implemented. The results of this study should be compiled shortly.

The Department of Homeland Security, in particular CBP, is committed to providing security for our nation without impeding the free flow of commerce. The FY 2005 President's Budget should provide CBP with the flexibility to align our staff to existing workload and provide services where needed.

Post-Hearing Questions for the Record
Submitted to the Honorable Tom Ridge
From Senator Susan Collins

"The Department of Homeland Security's Budget Submission for Fiscal Year 2005"

February 9, 2004

Unmanned Aerial Vehicles

1. Secretary Ridge, the Fiscal Year 2005 budget includes $10 million to develop, procure, deploy, and operate unmanned aerial vehicles to support the Bureau of Customs and Border Protection. This technology could help DHS meet its goal of creating a virtual border. In fact, one company in Maine, the Telford Group Inc., has been developing and testing this technology. Using advances already made in this area could possibly lower the costs to the taxpayer. Will the Department use these funds to support private sector research, development, and testing of unmanned aerial vehicle technologies?

Answer: Unmanned aerial vehicles (UAVs) in combination with their on-board sensors are particularly useful for monitoring remote land border areas. The high endurance of the larger classes of UAVs permits uninterrupted overnight or around-the-clock coverage, and the size and operating altitudes can make UAVs effectively undetectable by unaided human senses. The UAV's ability to provide communications links for coordinating multiple units on the ground is important in remote border operating areas. Operations in remote areas also are relatively easy to deconflict with local air traffic and communications frequencies. UAVs operated in support of border security can be focused in regional areas to minimize the number of operating sites and communications links to be acquired, operated and maintained; thus minimizing mission costs.

Much of the early development of UAVs has taken place in a military context with DOD flying UAVs in the National Air Space as a means of testing and evaluating their performance prior to deploying them in conflict scenarios. Technological advancements in the design and operation of UAVs have led to an increasing awareness of the potential for non-military use.

There are many government-funded UAV research and development (R&D) projects. The Customs and Border Protection UAV initiative is not focused on R&D, but rather to identify, acquire and deploy proven, commercial off-the-shelf UAV systems that can be immediately used in the border security environment. Existing government contract mechanisms, such as the DoD Joint Unmanned Aerial Vehicle Program, will provide pre-competed government contracts to efficiently and quickly acquire proven UAV systems at a lower cost to the taxpayer.

Fire Act Grants

2. I strongly support the FIRE Act grant program, which has helped communities across Maine and the United States. As you know, I have proposed legislation that would preserve the structure of the FIRE Act, and make sure the fire service continues to play a key role in its administration. While FIRE Act grants have been moved from FEMA to ODP, are you committed to preserving the structure of this program? In particular, will the Department continue to make grants directly to Fire Departments and involve the fire service in reviewing the applications?

Answer:

Let me assure you that the Administration and the Department of Homeland Security (DHS or the Department) are committed to providing our nation's first responders, including those in the fire service, with the resources, training, and assistance needed to accomplish their critically important mission. As part of this effort, the Administration and DHS continually strive to provide funding, assistance, and support in the most efficient and effective manner.

For several years, numerous first responder agencies and first responders have called for a single Federal point-of-entry that would consolidate and integrate disparate Federal preparedness initiatives into a more streamlined program. The decision to move the administration of the Assistance to Firefighters Grant Program (Fire Act) to DHS's Office of State and Local Government Coordination and Preparedness (OSLGCP), which includes the Office for Domestic Preparedness (OSLGCP) from the Emergency Preparedness and Response (EP&R) Directorate is part of the Department's efforts to provide first responders a "one-stop shop" for grants and other forms of assistance.

DHS appreciates your efforts to reauthorize the Assistance to Firefighters (Fire Act) Grant program, and is supportive of provisions that place grant authority with the Secretary of Homeland Security, expand eligibility for emergency medical services, and adjust award amounts based on city size. However, the Department has concerns about provisions covering the role of fire service organizations, as these may change current administrative practices and limit programmatic flexibility.

As currently drafted, this legislation constrains the Secretary's authority to exercise oversight over the grant process by providing overly broad authorities for non-Federal organizations to determine grant criteria and funding allocations. While DHS highly values the expertise and advisory input of national fire service organizations into the AFG program, this section could be

interpreted as delegating Federal policy decisions and appointments to non-governmental entities. Directing that "a national organization" will appoint the grant review panel, rather than the Secretary, is particularly objectionable. This section should be modified to clarify that input from non-governmental entities on Federal appointments and expenditures will be advisory, as it has been in the past.

The President's FY 2005 Budget request for the Assistance to Firefighters Grant Program includes language that would give priority to applications enhancing terrorism preparedness. This is consistent with Homeland Security Presidential Directive (HSPD)-8, which establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies. As the Assistance to Firefighters Grant program will play a critical role in strengthening preparedness capabilities of States and localities, DHS will continue to adhere to HSPD-8 by emphasizing terrorism preparedness while continuing to support all-hazards preparedness. The Administration considers this critical to implementing the 9/11 Commission's recommendation on homeland security assistance. While DHS does not believe this legislation would hamper this effort, it would prefer that terrorism preparedness considerations to be noted as part of this program's objective.

In the meantime, OSLGCP has managed the AFG program consistent with report language accompanying the FY 2004 appropriations by convening numerous meetings and is working closely with officials from EP&R and the U. S. Fire Administration. As in past years, fire department officials will be involved in the peer review process and fire departments will apply and directly receive awards from OSLGCP.

Coast Guard R&D Question

3. The Coast Guard has for many years maintained a vibrant research and development program. For example, the Coast Guard R&D Center in Groton, Connecticut has worked closely with the University of Maine in developing a durable, weather resistant wood composite building material for use in harsh marine environments. Now that the Coast Guard's R&D program and budget has been absorbed by the Department's Science and Technology Directorate, how do you intend to maintain a specialized emphasis in the area of maritime science and research?

Answer: The Department is mindful of the requirements of section 888 of the Homeland Security Act of 2002. The Science and Technology Directorate (S&T) and Coast Guard (CG) are in the midst of preparing a formal agreement that will detail the coordination and funding mechanisms for CG R&D capabilities. The foundation for that agreement will be the consolidation of funding requested in the FY2005 budget. For FY 2005, the CG R&D center facility, personnel and maintenance expenses will be funded through S&T in the amount of $13.5 million. In addition, S&T and the CG have agreed upon a base level of additional project funding in the amount of $5 million that will be specifically targeted toward non-security related projects including maritime science and research. This funding will be designed to support CG mission-programs such as Marine Environmental Protection, Living Marine Resources, Search

and Rescue, Aids to Navigation and Marine Safety. The specific projects in support of these mission-programs will be prepared annually for S&T concurrence.

In addition to this $18.5 million in funding, the Coast Guard will submit security-related research requests through S&T for coordination across all portfolios and DHS components. The Coast Guard has submitted a maritime security R&D portfolio detailing approximately $50 million in vital maritime security research initiatives. This portfolio has been validated by S&T portfolio managers and will be considered in the development of future spending priorities and commitments from S&T.

This integration of funding and effort will go far to minimize redundancy and maximize the effectiveness of Coast Guard R&D while ensuring that all Coast Guard mission requirements remain a key part of S&T planning and resource decisions.

Post-Hearing Questions for the Record
Submitted to the Honorable Tom Ridge
From Senator Tom Carper

"The Department of Homeland Security's Budget Submission for Fiscal Year 2005"

February 9, 2004

State First Responder Grants

a) The President's FY05 budget proposes allocating first responder grants to states "based on population concentrations, critical infrastructures, and other significant terrorism risk factors, as determined by the Secretary of Homeland Security." This appears to abandon the formula included in the USA PATRIOT Act. While I believe the PATRIOT Act formula should be modified so that a state's allocation is based in part on actual risks and vulnerabilities, I am concerned that the President's proposal would not guarantee that each state receives an adequate baseline funding amount. Will all 50 states receive funding under the President's proposal? Without a baseline requirement, how will you ensure that every state receives the resources necessary to achieve basic levels of preparedness?

Answer:

The President's Fiscal Year (FY) 2005 budget request includes $750 million for formula-based grants to the states and $500 million for law enforcement terrorism prevention grants, which continues the Administration's and DHS' support for our nation's emergency prevention and response community.

I have said consistently that I believe there should be a minimum level of preparedness across the country -- and that every state should receive some resources. However, dividing 40 percent of these funds evenly among every state simply leaves too little flexibility. The language in the President's FY 2005 budget request for DHS recognizes that other factors should be considered in addition to population in making the overall funding allocations and that the Secretary should have the discretion and latitude to make this determination.

The Administration has also said consistently that we supported more flexibility in the USA PATRIOT Act formula so that more funds can be allocated based on threats and vulnerabilities. As concentrations of critical infrastructure and politically attractive targets tend to increase threat levels dramatically, population is not the sole determinant of risk or vulnerability.

b) What are the "other significant terrorism risk factors" you would use to determine state allocations under the President's proposal? What role will the risks and vulnerabilities identified in state homeland security plans play in determining these factors? What role will classified intelligence play?

Answer:

As a requirement to receive their FY 2004 Homeland Security Grant Program funds, and additional funds in FY 2005, states conducted threats and vulnerabilities assessments and, based on that information, developed homeland security strategies. The states were required to provide completed homeland security strategies to OSLGCP by January 31, 2004. At this point, OSLGCP has received strategies from all the states and territories, the District of Columbia and the Commonwealth of Puerto Rico. OSLGCP and an internal DHS Review Board have approved a majority of these strategies. A few states and territories are working to provide additional information and details to finalize their strategies, but OSLGCP anticipates that all strategies will be approved in the next few weeks. These strategies are critical resources to the states in the efforts to distribute funds in the most effective manner to address the homeland security needs. They are also important because they will allow the Department to match the preparedness needs as outlined in the state homeland security strategies with resources available from the federal government. The information provided in these strategies will allow the Department to make informed decisions on how funds will be distributed and what factors the Department will use to make this determination.

Urban Area Security Initiative

c) I am concerned that the President's FY05 budget shifts funding for state first responder grants while more than doubling funding for the Urban Area Security Initiative (UASI), which will issue grants to "high threat, high density" urban areas. Many states, including my own, have received no money at all under the UASI. What is the rationale for this shift? If an increasing percentage of federal first responder will now be going to large urban areas instead of states, how will you ensure that states like Delaware will continue to receive the resources necessary to reach basic levels of preparedness?

Answer:

The Department and the Administration believe that all states and territories should receive a minimum level of funding. At the same time, the USA PATRIOT Act needs to be updated to allow more funds to be allocated based on threats and vulnerabilities. . To address both of these goals, the Department has administered dual funding programs -- a formula-based state minimum program and a high-threat, high-density urban areas program -- since FY 2003. The President's FY 2005 budget request supports broad-based funding for states and targeted funds for the nation's urban areas. In addition, the information provided by the states and territories in their homeland security strategies will help the Department determine the minimum levels of funding required to sufficiently address states' homeland security preparedness needs.

d) How will you determine which urban areas will qualify for UASI grants? What role will the risks and vulnerabilities identified in state homeland security plans play? What role will classified intelligence play?

Answer:

The funding distribution model used to allocate FY 2003 and 2004 UASI funds was based on a combination of three variables, which resulted in an assignment of a terrorist risk estimate for each city. The variables were: (1) a combined threat index derived from classified CIA and FBI threat data, along with the number of FBI terrorism cases opened in a region; (2) a count of critical public and private sector assets, weighted for vulnerability; and (3) population density. Each of these three variables was normalized and then weighted and summed to give an overall terrorist risk estimate. The Department likely will use a similar method to distribute funds made available for continuation of this program in FY 2005.

e) How does the Department ensure that preparedness efforts undertaken by localities receiving UASI grants do not duplicate or contradict efforts undertaken at the state level?

Answer:

In order to receive funds under UASI, urban areas are required to conduct urban area threat, vulnerability, and needs assessments and develop an urban area security strategy. These strategies must be provided to and approved by OSLGCP prior to the urban areas' receipt of their allocated funds.

As part of this effort, OSLGCP has required that each designated urban area convene an Urban Area Working Group (UAWG), which consists of representatives from the core city and core county as well as representatives from contiguous jurisdictions and mutual aid partners. The UAWG will be responsible for coordinating development and implementation of all initiative elements, including the urban area strategy development, the methodology for the allocation of funds (in coordination with the State Administering Agency (SAA)), and any direct services that are delivered by OSLGCP.

Funds provided under the UASI program largely are provided directly to the state within which the urban area is located. The states are required to pass-through at least 80 percent of the allocated funds to the designated urban area. The remaining 20 percent must be used by the state to benefit the designated urban area. In the event of a terrorist or mass-casualty incident, state assets will certainly be part of the response plan. Therefore, states are able to retain 20 percent of the allocated funds to support these types of activities.

Since these funds are provided to the state, the SAA for OSLGCP funds is a vital part of the UAWG. The SAA point-of-contact, in coordination with the UAWG, will develop a methodology for allocating funding available through the UASI. At a minimum, the core city and core county/counties must provide written concurrence on this spending plan.

Assistance to Firefighter Grant Program

a) The President's FY05 budget proposes changing the Assistance to Firefighters Grant Program so that funds could only be used for firefighter training and the purchase of fire vehicles, equipment and personal protective gear. This means that fire departments would no longer be able to apply for funding for a number of other important programs authorized by the FIRE Act. What is the rationale for this change?

Answer: The President's FY 2005 Budget request for the AFG program includes language that would give priority to applications enhancing terrorism preparedness. This is consistent with Homeland Security Presidential Directive (HSPD)-8, which establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies. As the AFG program will play a critical role in strengthening preparedness capabilities of States and localities, DHS will continue to adhere to HSPD-8 by emphasizing terrorism preparedness while continuing to support all-hazards preparedness. The clear majority of grants funds have and continue to provide training and equipment that are dual use in that they enhance both all hazard and terrorism preparedness. In addition, the Administration considers this critical to implementing the 9/11 Commission's recommendation on homeland security assistance.

b) As you may know, a recent review of the Assistance to Firefighters Grant Program by the Department's Inspector General suggests a greater emphasis should be placed on fire prevention and education. How do you plan to address the IG's concerns in light of the fact that the President's proposed budget would no longer allow FIRE Act grants to be used to fund fire prevention and education programs?

Answer: The authorizing statute requires us to provide a minimum of 5% of appropriated funds to fire prevention activities. It provides us with a specific authority to award fire prevention projects to non-fire department organizations as well. In the fall of 2004, the Department will provide fire departments and non-fire department community organizations recognized for their work in fire prevention with an opportunity to apply for grants that support fire prevention activities. It is our belief that the low level of requests for fire prevention projects demonstrated in the FY2004 March application period (only1%) can be turned around by applying grant writing technical assistance techniques similar to those of the March period.

c) As you may know, a leading cause of firefighter death in America is a heart attack occurring either at the scene of an emergency or soon after returning from an emergency. Firefighters getting lost inside burning buildings is another leading cause. How do you plan to address these issues in light of the fact that the President's proposed budget would no longer allow FIRE Act grants to be used to fund firefighter wellness and fitness programs or the creation of rapid intervention teams?

Answer: Rapid intervention teams (RIT) are created from the equipment and training provided to firefighters for carrying out the rescue operation inside the burning building. The Assistance to Firefighters Grant Program support for the development of RIT capability will continue, but rather than being cited as a separate activity, it is integrated into the equipment and training activities supported by the program. DHS remains committed to improving the health and wellness of firefighters through a number of initiatives managed by the U.S. Fire Administration. These initiatives include:

- Co-Sponsorship of a first-of-its-kind Firefighter Life Safety Summit in March 2004. This summit, co-sponsored by the National Fallen Firefighters Foundation and supported by FEMA and DHS brought together more than 200 fire and emergency services representatives from more than 100 organizations and departments. The summit attendees produced a preliminary report that detailed initiatives and recommendations for drastically reducing firefighter fatalities and injuries, including reducing the number of firefighters losing their lives due to disorientation inside burning buildings. In April, a follow-up meeting was held in Arizona to review the report and begin putting action behind the words.
- In partnership with the National Volunteer Fire Council, USFA recently developed and released the *Health and Wellness Guide for the Volunteer Fire Service.* This document provides detailed information and examples of effective health and wellness programs aimed at the needs of volunteer firefighters.
- Partnered with the International Association of Fire Chiefs, International Association of Fire Fighters, and the National Volunteer Fire Council to reduce the number of firefighters killed while responding to or returning from the emergency scene. These types of incidents, primarily vehicle crashes, have killed more than 225 firefighters in the line of duty over the last 10 years. These partnerships will take the recommendations from the recently completed Fire Service Emergency Vehicle Safety Initiative, which was jointly sponsored by the USFA and Department of Transportation Federal Highway Administration, and develop materials targeted at Chief Officers and Fire Department Leadership.

d) The President's budget also proposes increasing the award limit for Assistance to Firefighters grants going to fire departments serving "major" cities. How do you plan to define which cities qualify as "major" cities? By how much do you plan to increase award limits? Would these increases mean that fewer fire departments will receive FIRE grants? Will there be an effort to award more grants to fire departments serving "major" cities?

Answer: The President's budget request would allow fire departments serving populations above 500,000 to qualify for grants not to exceed $2 million. Grant awards under the FY 05 Assistance to Firefighters Grant Program will continue to be subject to peer review and recommendation. It is difficult to predict the recommendations of the peer review process and thus equally difficult to know whether there may be more or

fewer grant awards to departments serving a given population.

Information Sharing

I learned recently that, when the terrorism threat level was last raised from yellow to orange last December, the Department sent a list to each governor of the critical sites within his or her state that required additional protection. Delaware's list consisted of seven sites, including a chemical facility that was no longer in operation. I'm told that a number of states had similar problems with their lists. How much, if any, input did individual states have in compiling these lists? How did you determine what to place on them? Are you aware that some lists included outdated information? What is being done to ensure that more accurate information will be used the next time the terrorism threat level is raised?

Answer:

As you noted, on approximately December 23, 2003, the states were provided a list of their critical assets in connection with the elevation of the national threat level from "Yellow" to "Orange" to ensure that appropriate protective measures could be adopted. Those assets were drawn from the Department's Protective Measures Target List (PMTL), which is exactly what the name implies—a list of those sites across the nation that we consider potentially most attractive to terrorists. Some states also were provided additional criteria. The data that was furnished to the states in December was from the Department's initial effort to assemble the PMTL in October 2003.

With respect to issues regarding the quality of the PMTL and other databases, we are fully aware of some errors and omissions. Those databases were established and compiled from multiple sources, including the states themselves, and we are working to identify gaps, errors, and duplicate entries and to eliminate outdated entries. This has been a high priority for the Department since November to December 2003. Consequently, the PMTL undergoes continuous refinement and improvement. In late February 2004, the Department's Information Analysis and Infrastructure Protection (IAIP) Directorate sent a letter to all state homeland security advisors that contained the list of approximately 1,700 sites in the PMTL and asked for any updates, changes, or additions. State inputs are now being received and integrated.

Post-Hearing Questions for the Record
Submitted to the Honorable Tom Ridge
From Senator Peter Fitzgerald

"The Department of Homeland Security's Budget Submission for Fiscal Year 2005"

February 9, 2004

CFO Act

On August 1, 2003, Senator Akaka and I introduced S. 1567, the Department of Homeland Security Financial Accountability Act, which would improve the financial management of the Department of Homeland Security by including the Department under the Chief Financial Officers Act (CFO) of 1990. Senators Levin, Nickles, Lieberman, and McCain also are cosponsors of the bill.

The CFO Act requires the submission of annual audited financial statements and performance and accountability reports; it requires the CFO to be appointed by the President and confirmed by the Senate; and it also requires that the CFO report directly to the Secretary. Although the Department of Homeland Security is the third largest department in the federal government, it is the only cabinet-level department that is not covered by the CFO Act.

In testimony before this committee, the Comptroller General of the United States, David Walker, stated that the Department of Homeland Security should be included under the CFO Act and that S. 1567 should be passed and enacted as expeditiously as possible.

On November 21, 2003, the full Senate passed S. 1567, as amended, by unanimous voice vote. In addition, the House Government Reform Committee and the House Select Committee on Homeland Security also favorably reported the companion House bill.

1. Secretary Ridge, do you support including the Department of Homeland Security under the CFO Act?

Answer: Pursuant to PL 108-330, DHS is now a CFO Act agency and will comply with the requirements of that Act.

2. What additional steps will you take to strengthen and improve the Department's financial management and help eliminate the potential for waste, fraud, and abuse?

Answer: DHS will hold a Department-wide Financial Management Conference from February 1st – 4th, 2005. This conference will fully discuss DHS' requirements as a CFO Act Agency; form an Internal Control Committee to oversee the upcoming internal control audit; review and explain key programs including Working Capital Fund and Purchase Card; and stress the need for bureaus to resolve weaknesses identified in the FY 2004 DHS Performance and Accountability Report (PAR).

DHS is stepping up its compliance with the Improper Payments Information Act (IPIA). A recovery audit contractor is analyzing disbursement data received from CBP and ICE with the goal of identifying improper payments. DHS is undertaking a statistically verifiable sample of each bureau's largest IPIA program to support the results of an IPIA risk assessment that was reported in DHS' FY 2004 PAR.

The CFO is about to distribute a memo to bureaus CFOs which will give bureaus until December 31, 2004 to submit detailed corrective action plans, including key milestones, for all internal control weakness identified in DHS' FY 2004 PAR.

Finally, the CFO has hired a career Deputy CFO who will join DHS after the year end holidays.

Departmental Management

The Department of Homeland Security (DHS) is the third largest department in the federal government with a budget of over $30 billion for fiscal year 2004. In addition, the Department inherited 22 components with 19 different financial management systems and 15 compensation systems. In order for this department to be successful, it must have sound financial systems and rigorous independent audits.

In January 2003, the General Accounting Office (GAO) included the Department of Homeland Security on its High Risk List, citing a number of major management challenges and program risks.

1. When you last appeared before this Committee in May 2003, you stated that the Department of Homeland Security was reviewing the GAO's recommendations regarding fiscal management, and was going to work to strengthen areas and systems of weakness as the consolidation process moved forward. Since then, what progress has been made in strengthening financial management practices throughout the Department?

Answer: Based on the recommendations from the FY 2003 audit, the Department will be receiving action plans from each component that will address their material weaknesses, and outline the major steps, including milestones that the component will take to correct these weaknesses. The CFO will monitor the status of these corrective actions through monthly Clean Actions Plan (CAP) meetings.

2. What specific duplicative or unnecessary functions have you identified within the Department? If so, how are you working to eliminate them?

Answer: The Department is working to identify and reduce the number of disparate finance, accounting, information technology, procurement, and administrative processes and systems. In FY 2003 the Department inherited 22 components with 19 different financial management systems. In the past year the Department has consolidated into 10 different financial systems and we are working to further reduce that number as we move into FY 2005. The FY 2005 budget

includes $49 million provided for the design, development and implementation of a single Department-wide financial management system. It will provide decision-makers with critical business information, e.g., budget, accounting, procurement, grants, assets, travel, in near "real-time"; eliminate stovepipes between, and within, components; migrate, modernize, and integrate DHS business and financial processes, policies, and systems; and, identify opportunities to establish common: (i) information-sharing practices; (ii) business practices; and (iii) architecture.

Through our integration process, the Department has eliminated the need for each component to produce financial statements and enter data into the Financial Management System (FMS) FACTSI, and FACTSII systems. The Department is using an application that consolidates accounting data from all the components and generates the necessary reports to produce the financial statements enabling the headquarters office to send consolidated bulk data to FMS.

The Department received $36 million in FY 2005 to invest in the design, development and implementation of a new human resource information system. This will support DHS efforts to move toward an integrated HR information technology for consolidating the existing disparate systems and implementing e-Gov solutions.

Similarly, the Department has been able to consolidate 13 separate contracting offices from detached legacy organizations to draw together a procurement program comprised of eight component organizations. In addition, 22 different human resource servicing offices have been consolidated down to seven and the Department has consolidated eight different payroll systems currently down to three and will be using one single payroll system by the end of the year.

As part of our merger and acquisition efforts, the Department conducted a business transformation by realigning over 6,000 support services employees (both government and contractor) from the legacy U.S. Customs Service and the legacy Immigration and Naturalization Service to support the 68,000 employees of the U.S. Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and Citizenship and Immigration Services (CIS) organizations. To accomplish the transformation, an Integrated Working Group (IWG) was established comprised of the service providers and the mission elements. The IWG devised service plans for seventy different service categories using a shared services concept with one mission element providing a service to the other two participation elements. Best practices, efficiency and effectiveness were studied to determine the best approach for the provision of each service. The group developed metrics driven resource allocation algorithms to reallocate the 6,000 support spaces to match the service requirements. The participating agencies then entered into Service Level Agreements (SLAs) for the shared services.

What steps are you taking to ensure that the process of integration occurs as quickly as possible and ensures effective and efficient management of the Department's operations? When do you expect the Department to be fully integrated?

Answer: The integration of the Department is a critical step in making DHS a 21st Century Department. To that end, the Department has identified that integration can only be realized through the harmonization of all of the Department's business processes associated with its operations and determining the most effective and efficient process that is to be incorporated for

each particular line of service. Additionally, the appropriate information technology support and infrastructure must also be utilized and aligned to support these shared services based upon best business decisions and a focus on delivering the services to our mission-oriented frontline employees,

The current CFO plan for functional integration is a phased implementation moving towards a "centers of excellence" model. This approach focuses on four main tracts leading towards shared services: multiple systems, multiple processes, multiple organizations and multiple locations. The CFO intends to strategically initiate efforts in the areas of multiple organizations, processes, and systems.

In order to address the integration of processes and organizations, the CFO Intends to initiate direct links from the DHS CFO to the equivalent positions within the components. The CFO also intends to be involved immediately in senior level (i.e., SES) hiring, performance evaluation and compensation decisions. Furthermore, we are contemplating creating similar links in the areas of financial management and budget to the directors of the Financial Management and Budget offices within the OCFO.

The systems tract will be addressed primarily through a resource transformation initiative entitled ***eMerge²***. The goal of ***eMerge²***, which stands for *"electronically Managing enterprise resources for government effectiveness and efficiency"*, is to improve resource management and enable the bureaus to move "Back Office" effectiveness and efficiency to "Front Line" Operations. ***eMerge²*** is a business-focused program that seeks to consolidate and integrate the Department's budget, accounting and reporting, cost management, asset management, and acquisitions and grants functions. Once procured and developed, the solution will be rolled out in several phases focusing first on those organizations most in need of improved basic financial management services. ***eMerge²*** is currently in the midst of an exhaustive requirements definition and design phase, which is expected to evolve into a solutions acquisition phase this summer. As ***eMerge²*** is implemented over the next few years, it will greatly enhance Departmental visibility, oversight and accountability of component operations and financial management.

The timeline for ***eMerge²*** is:

- FY04 – Selection & Pilot
- FY05-06 – Implementation Rollout
- FY07 – All agencies using the ***eMerge²*** Solution

Additionally, in support of this effort to integrate, the Department has, in just four months, accomplished something unique in the Federal Government – the design and delivery of a comprehensive and immediately useful target Enterprise Architecture (EA). The target Enterprise Architecture is both a conceptual model and an actionable process for managing change across the enterprise. The EA provides the vision, concepts and structure to enable, enhance and increase the efficiency and integration of DHS. By doing so, the Departmental EA will be able to highlight overlapping, duplicative initiatives and identify financial inefficiencies, resulting in cost savings for US taxpayers.

The second version of the EA, due to be released in September 2004, will further align information technology investments with mission and business needs and improve data sharing and interoperability with DHS partners.

Nuclear Power Plant Security

My home state of Illinois has eleven operating nuclear power plants – the most of any state in the nation. These facilities provide 51.6% of the electricity generated in Illinois. The security of nuclear power plants is therefore important not only because of the potential damage a terrorist attack could cause, but also because nuclear power plants are a major source of energy in my state.

On November 8, 2003, the *Washington Post* published an article regarding an alert from the FBI and the Department of Homeland Security, warning that al Qaeda operatives may attempt to hijack cargo planes in neighboring countries and fly them into nuclear plants in the United States. Two of the plants in Illinois are three hundred miles from our northern border.

The President's February 2003 *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* specifically addresses the role of the Department of Homeland Security in coordinating security efforts with nuclear power plant owners and operators.

a) In May of last year when you last appeared before this committee, I raised with you the issue of nuclear power plant security. At that time, you stated that your Department worked closely with the Nuclear Regulatory Commission and the Federal Bureau of Investigations (FBI) to enhance security at these power plants. Since that time, there have been increased threats against our plants. What steps have been taken since we last discussed this issue to protect the nation's nuclear plants?

Answer:

In July of last year, IAIP developed two reports on nuclear power plants: (1) Characteristics and Common Vulnerabilities Report; and (2) Potential Indications of Terrorist Activity Report. Those reports are made available to owners and operators of nuclear power plants. The Characteristics and Common Vulnerabilities Report informs owners and operators of the most likely ways in which a terrorist might seek to attack their site. This is a crucial step in better preparing the defense of a nuclear power plant. The Potential Indications of Terrorist Activity Report contains observations indicating the possibility of the formation or existence of a terrorist plan to attack or sabotage a facility. This can assist owners, operators and security personnel in identifying a specific asset a terrorist group might target, the general or specific timing of a planned attack, and the weapons and deployment method planned by the attackers. Both of these reports help improve the security of facilities that already represent a substantially hard target for terrorist attack.

In addition, DHS is represented on the White House Homeland Security Council's interagency Policy Coordinating Committee on Commercial Nuclear Power Plant Security. This

organization is chartered to enhance integrated security response planning at these facilities. FBI, DoD, and the NRC also participate in the PCC.

Finally, a pilot program is underway at the Millstone Nuclear Power Plant (Millstone) in Connecticut to develop anti-intrusion water barriers. The Department is working with the Nuclear Regulatory Commission (NRC), Millstone, the U.S. Coast Guard, and state and local entities on this project. Determination of future locations for such barriers and associated funding and identification of partners to expand this project to include other plants have not yet been determined.

b) How would you improve the development and implementation of security programs to protect nuclear power plants?

Answer:

Nuclear power plants are representative of an industry with a long-standing and active protective security history and culture. In addition to already stringent security requirements, plants owners and operators and local law enforcement will further improve plant security through implementation of Buffer Zone Protection Plans (BZPPs). Those plans are used to determine ways to further reduce vulnerability to terrorist attack by addressing the area of land that surrounds the property associated with the nuclear power plant. An exercise has been conducted at the Calvert Cliffs Nuclear Power Plant and there are plans to do several more. BZPP templates have been made available to all nuclear plant owners and operators.

In addition, DHS is developing plans for and deploying Protective Security Advisors (PSAs). Each PSA will have responsibility for a specific region of the country and will maintain a close relationship with nuclear power plant owners and operations in their specific area of responsibility. PSAs will facilitate information sharing, organize protective security training, assist in emergency coordination, and represent DHS in the communities in which they are posted. Security Augmentation Teams (SATs) are also being developed that will consist of about 25 personnel who are drawn primarily from major urban SWAT units. SATs will focus on protecting high-value sites (such as nuclear power plants), develop working relationships with the site's permanent protective security team, and become familiar with the site's specific vulnerabilities. The PSA and SAT programs are still in their early stages but are being actively pursued by the Department.

c) What are your plans to ensure the Department of Homeland Security is working with the private companies that operate these plants to verify that employees are fully trained for the increased security responsibilities they now face?

Answer:

The Department believes the NRC is better positioned to answer this question owing to its overall regulatory responsibilities. DHS is prepared to assist the NRC in building protective security capacity in the nuclear power plant industry as part of its larger efforts to protect critical infrastructures from terrorist attack.

d) Do you think that the current allocation of responsibilities and protective efforts among the Department of Homeland Security, the Nuclear Regulatory Commission, state and local law enforcement, and the private sector is sufficient?

Answer:

Yes, the current allocation of responsibilities and protective measures is appropriate. The NRC's long history of working closely with industry, its technical prowess, and clear regulatory role best position it to effectively oversee security issues occurring within the confines of a nuclear power plant. In support of this role, the recently signed Homeland Security Presidential Directive #7 (HSPD-7) provides a sound framework for coordination across Federal agencies, with state and local authorities, and the private sector to protect nuclear power plants. Under HSPD-7, DHS works closely with the NRC and the Department of Energy, when appropriate, to protect commercial nuclear reactors used for generating electric power and non-power nuclear reactors used for research, testing, and training. DHS also collaborates with NRC on the security of nuclear materials in medical, industrial, and academic settings and in the transportation, storage, and disposal of nuclear materials and waste. A key objective for DHS is increasing the cross-sector communication among these groups to understand common vulnerabilities, protective measures, and best practices.

Agriculture Security and Bioterrorism

My home state of Illinois is one of the most agriculture-dependent states in the nation. Illinois has approximately 78,000 farms utilizing nearly 28 million acres, which is about 80 percent of the total land area. Additionally, the food and fiber system in Illinois employs 1.5 million workers. Agriculture and agriculture-related industries form the backbone of my state and many others, and an attack on any aspect of the industry's long production and supply chain could cause incredible economic disruption.

The Canadian press issued a report on November 11, 2003, regarding a Canadian intelligence warning that al Qaeda operatives may poison Canada's food or water using ricin, botulinum toxin, or other poisons.

1. How serious is this threat and do you believe a similar attack is likely in the United States?

Answer: Our understanding is that there was in fact no intelligence referring to a specific threat, as suggested by the article that the Canadian press issued on November 11, 2003, regarding a Canadian intelligence warning that al Qaeda operatives may poison Canada's food or water using ricin, botulinum toxin, or other poisons. (for reference, the Canadian press article (dated November 12, 2003) is available electronically at: www.ctv.ca/servlet/ArticleNews/story/CTVNews/1068644517552_24 (27 February 2003).

The report, entitled 'Ricin and Botulinum: Terrorist Use of Toxins', was prepared by the Canadian Privy Council Office's intelligence assessment secretariat, and issued in February 2003. It considered possible scenarios for the illicit use of these toxins, e.g., what might happen,

what vulnerabilities might exist, etc. The fact that the Canadian Privy Council Office studied this scenario is not evidence they had intelligence referring to a specific threat.

2. If such an attack occurred in Canada, how might the American food chain and water supply be affected?

Answer: If such an attack were to occur in Canada, we would not expect any significant effect on the United States water supply. Contamination of large water supplies, such as reservoirs, is extremely difficult due to the volume of contaminant required and down stream processing of the water. There might be some impact if processed foods were contaminated and then shipped into the United States. However, these processed foods would be consumed at varying times and at the initial signs of consumer illness, the remaining 'stock' of these items would be recalled, thereby limiting the extent of the negative health impact.

3. What additional precautions are you pursuing to protect against threats to our food and water supplies?

Answer:

The Department is pursuing a number of initiatives to protect against threats to our food supply, working closely with our partners at the Departments of Agriculture (USDA) and Health and Human Services (HHS) and in conformance with the agricultural and food security policies and responsibilities outlined by the Administration in Homeland Security Presidential Directive #9 (HSPD-9). Our protective measures focus on expanding vulnerability assessments of the food and agricultural sector as well as developing and implementing mitigation strategies to protect vulnerable nodes of food production and processing. We are also working with our Federal partners to improve detection of an event, threat prioritization, incident management, communications, and recovery efforts across the food and agricultural sector.

Through the Department's work with USDA and HHS, we are improving common screening and inspection procedures for food and agricultural items entering the United States and for domestic inspection activities. Evidence of our efforts can be seen at the nation's ports of entry, particularly those where the agricultural industry imports large volumes of plants, fruits, vegetables, meat, and other products. DHS agricultural specialists provide technical expertise to complement the work being done by food inspection officers, who receive training from USDA.

DHS also is working closely with the private sector to bolster information sharing mechanisms across the food and agricultural sector. As a highly diverse sector, ensuring timely communications to detect or manage a food event is crucial. Over the past several months, DHS participated in several discussions with the original Food Information Sharing and Analysis Center with the goal of expanding its scope to cover the entire infrastructure. DHS also is planning to lead a series of sector-wide meetings in conjunction with USDA and HHS and is studying new methods to detect the intentional introduction of catastrophic diseases in the food and water supply and developing prevention technologies.

To improve the security of our water supply, HSPD-7 designates the Environmental Protection Agency (EPA) as the sector-specific agency for coordinating protection efforts within the water sector. DHS leverages EPA's expertise and relationships to conduct joint vulnerability assessments of the infrastructure supporting drinking water, waste water, and water treatment facilities.

The President's February 2003 *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* discusses a cooperative initiative between state and local governments, industry, and the Departments of Homeland Security, Agriculture, and Health and Human Services to evaluate overall security and address existing vulnerabilities.

> How are you ensuring that the Department of Homeland Security is working effectively with state and local agriculture officials to develop a comprehensive security plan to protect the supply chain?

Answer:

This is a topic of personal interest to me and I have made the protection of the food supply chain a high priority. It is an integral component of the National Plan for Critical Infrastructure and Key Resources Protection. My Department is leading this and other planning efforts that include significant roles for our state and local partners. When completed, these efforts will allow us to provide the nation a comprehensive security plan for the food supply chain. We are also working with USDA, HHS, EPA, and the Attorney General to integrate food-specific standardized response plans into the National Response Plan.

Cost Effectiveness

Since you last appeared before this Committee on May 1, 2003, two new intelligence centers, the Terror Threat Integration Center (TTIC) and the Terrorist Screening Center (TSC) have opened. The director of TTIC reports directly to the Director of Central Intelligence, while the TSC reports to the FBI. The Department of Homeland Security, however, is responsible by statute for the analysis and dissemination of the information contained in these centers.

1. Given the role of DHS, would it be more cost effective and efficient to place the TTIC and the TSC under the direction of the DHS?

Answer:

As stated in the Homeland Security Act of 2002, DHS is responsible for threats to the Homeland. IAIP independently analyzes threat-related information it receives from the entire Intelligence Community, other DHS entities, and the Terrorist Threat Integration Center (TTIC), and issues warning products to state and local officials and the private sector after matching terrorist threats and intentions with our nation's vulnerabilities.

In contrast, the TTIC is a central point to which Intelligence Community members send all threat-related information. TTIC uses this information to create an overall threat picture and to issue reports to the appropriate Intelligence Community (IC) members. Similarly, the Terrorist Screening Center (TSC) provides information to and receives inputs from multiple members of the IC, as well as to and from state and local officials. Although TTIC and TSC are essential resources upon which DHS relies to complete its mission, they are also integral to completing the mission of other entities within the IC.

2. How does DHS currently work with these centers to ensure full coordination and cooperation?

Answer:

The IAIP mission is to enable, develop, and sustain the capability to continuously identify, assess, and prioritize current and future threats to the homeland, map those threats against vulnerabilities, issue timely warnings, provide the basis from which to organize protective measures to secure America, and assist in coordinating the response and restoration of critical infrastructure functions. This includes working with its fellow IC members and DHS entities to receive information directly and with TTIC to receive the appropriate reports regarding the broad threat picture. IAIP also has access to and participates in the watchlists consolidated at the TSC (in addition, intelligence analysts at DHS currently access information on suspicious persons by searching each individual list). In both cases, DHS has representatives located at the centers who are charged with ensuring the Department receives the appropriate information regarding the current threat picture, as well as information regarding any possible coordination and cooperation difficulties. DHS is in close and constant communication with these centers.

Recent news reports have raised concerns that as a nation we are unprepared to respond to acts of bioterrorism and that there is a lack of guidance and coordination among all levels of government.

a) What efforts are underway among the Department of Homeland Security, Health and Human Services, and other agencies to establish standards to guide federal, state, and local cooperation in preparing their response to bioterror attacks?

Answer:
The Department of Health and Human Services, through cooperative agreements administered by CDC and HRSA, has provided over $4.4 billion to States and cities since 2001 to bolster their preparedness to respond to bioterror attacks. Over $1.3 billion has been proposed in the FY 2005 budget for this purpose. These funds are associated with specific preparedness benchmarks to guide State and local preparedness efforts. An example of a specific benchmark is the Cities Readiness Initiative (CRI), which assists cities in the development of plans to distribute antibiotics to their entire population within 48 hours of a catastrophic bioterrorism attack.

The Department of Homeland Security has a number of joint efforts to establish standards and develop guidelines for federal, state, and local cooperative response to bioterror attacks. One example is an interagency effort to develop evaluation standards for biological detection devices. Participants in the working group include the Department of Health and Human Services' (HHS') Centers for Disease Control and Prevention (DHHS-CDC), the Food and Drug Administration , Department of Justice-Federal Bureau of Investigation (FBI), Department of Defense (DoD), the National Institute for Standards and Technology (NIST), and the Association of Analytical Communities (AOAC). This group, working in cooperation with the leading domestic manufacturers of detection devices currently marketed to the Nation's first responders for hand held field detection of *Bacillus anthracis* (Ba), are providing for the development of standards and testing as part of the process in defining these standards. These tests and standards will allow manufacturers to anticipate the performance characteristics that will be considered minimally acceptable for Ba testing as well as provide baseline information for first responders to use in selecting devices for field use. It is anticipated that these test results, and more importantly the system for future scientific testing evaluation, will be available by the end of this fiscal year.

Another effort is the development of a standard guide for a hospital preparedness plan to address the response to a bioterrorism event. This effort is being managed through the American Society for Testing and Materials (ASTM) committee on homeland security with members from academia, HHS, DHS, NIST and others.

The Department of Homeland Security is also facilitating the exchange of historical testing information between the DHHS-CDC and FDA, and DoD on tests used for biological threat agent environmental detection and clinical diagnosis. This data exchange will provide public health decision makers with a better understanding of the implication of test results when assessing the risk to public health. In addition, this effort will provide the framework for recommendations on future collaborative studies to enhance understanding of the comparability of multiple tests when used in environmental monitoring and clinical diagnosis. By understanding how the different tests compare when performed on the same material by the full range of Federal agencies in routine environmental surveillance activities or in response to a biological event is essential for government officials to make appropriately informed decisions in a timely manner. The initial exchange of testing results and comparability assessments for biological threat agents within the Nation's civilian Laboratory Response Network (LRN) and the domestic DoD programs will be done during FY 2004.

A smaller but significant effort is the DHS-sponsored DoD/Defense Threat Reduction Agency (DTRA) BioNet program. The program seeks to improve the ability of a major urban area in the United States to manage the consequences of a biological attack on its population and critical infrastructure by integrating and enhancing currently disparate military and civilian detection and characterization capabilities. Consequence management guidance which informs the local, state, and federal response following an environmental monitor signal, is currently under development and initially will be deployed in cities operating the DHS BioWatch system.

b) Due to the number of agencies involved in this coordination effort, there exists the opportunity for bureaucratic overlap and duplication of effort. How does the current process promote the efficient use of homeland security resources in this area?

Answer: The Homeland Security Council focuses the federal agenda on key areas in homeland security and identifies the policy level strategic vision. With interagency input, national-level gaps are identified and agency mission-related prioritization occurs for gap filling. . Through the Policy Coordination Committee (PCC) process, HSC ensures that homeland security policies are developed and executed with interagency coordination, in order to minimize duplication of efforts.

Through the Office of Science and Technology Policy (OSTP), a number of scientific working groups related to the biothreat have been convened whose membership include representatives from the interagency community. By identifying areas of programmatic similarity, collaborative efforts are undertaken to leverage existing programs, thus preventing duplication of effort. Furthermore, these interagency working groups strategically plan and prioritize efforts of common interest so future agency activities will be complementary but not duplicative. One example is the OSTP Diagnostics Working Group whose members are identifying threat agent detection assay gaps and jointly prioritizing future research in this area to the benefit of the agencies.

Other efforts evolve out of more informal routes when agencies working in a particular area convene working groups in an effort to leverage on-going or planned activities. For example, DHS and DoD both have environmental monitoring initiatives which operate concurrently in some United States cities. By identifying the similarities, an integrated system can be deployed and a unified, coordinated response to a bio-attack initiated more rapidly. .

Post-Hearing Questions for the Record
Submitted to the Honorable Tom Ridge
From Senator Robert Bennett

"The Department of Homeland Security's Budget Submission for Fiscal Year 2005"

February 9, 2004

Critical Infrastructure Protection and Information sharing:

1. I am glad to see DHS making progress on implementing provisions that would protect critical infrastructure information voluntarily shared by the private sector. However, there seems to be some confusion about what protection critical infrastructure information received from ISACs will have. Could you clarify what the rule is and the rationale?

Answer: Protected Critical Infrastructure Information (PCII) received from Information Sharing and Analysis Centers (ISACs) will have the same protection as PCII received from the private sector. (Please see the attached Interim Rule for further information.)

2. I understand the protected critical infrastructure information program will be implemented in multiple stages. Could you estimate the length of time it will take for complete implementation?

Answer: The PCII Program is currently capable of receiving submissions from all of the critical infrastructure sectors. At the present time we are only accepting submissions in physical form, e.g., letters, CDs, tapes. We expect to be able to accept electronic submissions by the end of fiscal year 2004. Dissemination of PCII material by the Program Office is being implemented in three stages. In Stage 1, PCII material will be disseminated by the PCII Program Office only within IAIP. In Stage 2, PCII Material will be disseminated throughout DHS. In Stage 3, PCII material will be disseminated to other Federal agencies that want to participate in the program and to state and local governments that have signed a Memorandum of Agreement with the PCII Program Manager to participate in the Program. We expect to begin Phase 2 in fall 2004. We plan to begin Phase 3 in early 2005.

4. I continue to hear some frustration from critical infrastructure owners on getting threat information in a form that is useful. You mention in your testimony that you have made progress of the collection, analysis and sharing of critical intelligence with key federal, state and local entities. While that is an extremely important, I continue to be concerned about getting the private sector owners of our critical infrastructure threat information that would be helpful to them. Could you share your thoughts on that problem?

Answer: An essential element of homeland security is the protection of the nation's critical infrastructures by federal, state, local and private sector efforts. These infrastructures are the systems, assets, and industries upon which our national security, economy, and public health

depend. It is estimated that over 85% of the critical infrastructure is owned and operated by the private sector.

Recognizing that the private sector may be reluctant to share information with the Federal Government if it could be publicly disclosed, Congress passed the CII Act in 2002 with its provisions for protection from public disclosure. The Protected Critical Infrastructure Information (PCII) Program, established pursuant to the CII Act, creates a new framework which enables members of the private sector to voluntarily submit sensitive information regarding the nation's critical infrastructure to DHS with the assurance that the information will be protected from public disclosure. PCII may be used for many purposes, focusing primarily on analyzing and securing critical infrastructure and protected systems, risk and vulnerabilities assessments, and assisting with recovery as appropriate.

While we continue to work this issue and develop projects for implementation, DHS has initiated numerous programs that enhance the communication between the public and private sector. The majority of this responsibility resides with the Information Analysis and Infrastructure Protection (IAIP) Directorate.

IAIP works with multiple Information Sharing and Analysis Centers (ISACs) across the various sectors of industry. An ISAC consists of a secure database, analytic tools, and information gathering and distribution facilities that allow authorized individuals to submit either anonymous or attributed reports about information and physical security threats, vulnerabilities, incidents, and solutions. ISAC members also have access to information and analysis relating to information provided by other members and obtained from other sources, such as the US government and law enforcement agencies, technology providers, and the U.S. Computer Emergency Readiness Team (US-CERT), a public-private partnership in DHS that provides information on cyber security, cyber alerts, vulnerability notices, and other information. Each ISAC offers a confidential venue for sharing security vulnerabilities and solutions and facilitates trust between officials at the Federal, state and local level and the private sector. To allow sector coordination, the ISACs formed the ISAC Council in 2003 in order to work more efficiently with each other and with DHS to plan the evolution of their role in information sharing.

In addition, information is routinely shared through the Homeland Security Information Network (HSIN). The HSIN initiative is supported by the Joint Regional Information Exchange System (JRIES) that was originally developed by state and local authorities in partnership with the federal government. This system allows all states and major urban areas to collect and disseminate information between federal, state, and local agencies involved in combating terrorism. The network is a secure 24/7 real-time collaborative tool that has interactive connectivity with the Department's Homeland Security Operations Center. The US-CERT Portal is a component of the HSIN for cyber information. This secure system significantly strengthens the exchange of real-time threat information at the Sensitive-but-Unclassified (SBU) level to all users.

Recently, the HSIN initiative has been expanded to include critical infrastructure owners and operators and the private sector in the cities of Dallas, Seattle, Indianapolis, and Atlanta. The HSIN – Critical Infrastructure (HSIN-CI) Pilot Program is an unclassified network, which

immediately provides the Department's Homeland Security Operations Center with one-stop 24/7 access to a broad spectrum of industries, agencies and critical infrastructure across both the public and private sectors. This conduit for two-way information sharing provides the Department with an expanding base of locally knowledgeable experts and delivers real-time access to needed information.

Threat related information is routinely shared with the rest of the federal government through Homeland Security warning products and reports. Additionally, DHS, through better tearlines and protective measures provided by IAIP and through increased efforts at communication on the part of the Office of State and Local Government Coordination and Preparedness (OSLGCP) and the Office of the Private Sector, is communicating more and better information to state, local, tribal, major city, and private sector officials through Homeland Security Advisories and Information Bulletins than ever before.

To this end, unclassified information is shared through a daily Homeland Security Operations Morning Brief and the weekly joint DHS-FBI Intelligence Bulletin. SLGC also coordinates bi-weekly conference calls with all of the Homeland Security Advisors in all the states and territories to help relay important departmental information as well as respond to queries from advisors. The Department has also paid for and established secure communication channels to all of our state and territorial governors and their state emergency operations centers. This investment in communication equipment included secure VTC equipment along with Stu/Ste telephones. Additionally, DHS has worked to ensure every governor has been cleared to receive classified information and are working with the Governors and their Homeland Security Advisors to provide security clearances for five additional people who support the Governors' Homeland Security mission. This provides DHS an avenue for disseminating classified information directly to the location that needs the information.

Cybersecurity:

If you could provide the committee what you would consider DHS's accomplishments over the last year in the area of cyber security?

Answer: DHS's accomplishments over the last year in the area of cyber security fall in three broad categories: (1) the establishment of a national cyber security response system to address today's cyber issues; (2) the implementation of programs to promote information sharing and awareness, including coordinating efforts to secure the government's cyberspace; and (3) the development of longer term strategic initiatives to proactively address cyber security over the long term. Specific accomplishments in each of these areas include the following.

National Cyber Security Response System

Since the inception of National Cyber Security Division (NCSD) in June 2003, its primary efforts have been targeted towards building a national cyber security response system. The essential element of that objective, as articulated in the National Strategy to Secure Cyberspace ("the Strategy"), is a partnership between government and industry that is able to perform analyses, issue warnings, and coordinate response and recovery efforts.

To build such a system, NCSD established the U.S. Computer Emergency Readiness Team (US-CERT), a partnership between NCSD and the public and private sectors to make cyber security a national effort, increase public awareness of cyber threats and vulnerabilities, and improve computer security preparedness and response to cyber attacks. One key component of the US-CERT is the National Cyber Security Response System ("Response System") that was called for in the Strategy and represents a significant portion of the work of NCSD. The Response System provides for a nationwide, real-time, collaborative information sharing network that enables State and local government officials, Federal agencies, the private sector, international counterparts, and law enforcement entities to communicate and collaborate with DHS and each other on cyber issues. The Response System is made up of the following NCSD programs and initiatives:

- The US-CERT Operations Center

  The US-CERT Operations Center serves as a real-time focal point for cyber security. It is a 24x7x365 watch and warning capability that provides operational support for monitoring the status of systems and networks in order to provide a synoptic view of the health of the Internet on a continual basis and to facilitate securing those systems and networks. The US-CERT Operations Center has successfully incorporated the functions of the previously existing FedCIRC. In accordance with provisions of the Federal Information Security Management Act, US-CERT:

  - provides timely technical assistance to operators of agency information systems regarding security incidents
  - compiles and analyzes information about incidents that threaten information security
  - informs operators of agency information systems about current and potential information security threats and vulnerabilities.

  In addition, the US-CERT Operations Center conducts daily conference calls across U.S.-based watch and warning centers to share classified and unclassified security information, and provides daily information feeds to US-CERT's analysis and production functions. US-CERT also leverages information gained from the Cyber Watch Network established between the U.S., Canada, Australia, and the United Kingdom.

- The Homeland Security Information Network (HSIN)/US-CERT Portal

  The HSIN/US-CERT Portal ("the portal") is a secure, web-based collaborative system that enables US-CERT to share sensitive cyber-related information with government and industry members. The portal contains a set of tools that provide for alert notification, secure e-mail messaging, live chat, ongoing forum discussions, document libraries, and a contact locator feature. The portal provides instant access to the US-CERT Operations team, the US-CERT Cyber Daily Briefing containing a snapshot of the state of cyberspace, and updated cyber-event and other newsworthy information. The portal is

the cyber component of the overall DHS Homeland Security Information Network (HSIN).

- The US-CERT Control Systems Center

  The US-CERT Control Systems Center is the primary operational and strategic component of US-CERT's capability to improve the security of critical systems that control the Nation's infrastructure. This effort brings together government, industry, and academia to reduce vulnerabilities, respond to threats, and foster public-private collaboration across all types of control systems. Subject matter experts proactively analyze and assess vulnerability information and engage with specific control system vendors to raise awareness and share vulnerability information that may impact their products.1

- US-CERT public website

  A critical function of US-CERT is to provide government, private sector organizations, and the public the information they need to improve their ability to protect their information systems and infrastructures. The US-CERT public website is our primary means to provide this type of information to the public. US-CERT.gov contains relevant and current information on cyber security issues, current cyber activity, and vulnerability resources. The website also contains interactive forms to report cyber incidents and to register for the National Cyber Alert System (NCAS). Over 100,000 individuals visit the US-CERT.gov public web-site daily.

- The National Cyber Alert System

  The National Cyber Alert System (NCAS) is an operational part of the US-CERT Response System that delivers targeted, timely, and actionable information to Americans to allow them to secure their computer systems. Information provided by the alert system is specifically designed and targeted to be understandable to all computer users, technical and non-technical, and reflects the broad usage of the Internet in today's society. Over 270,000 users have subscribed to the system and are receiving regular alerts and updates. Since the launch of the system in January 2004, a total of 41 alerts have been issued to both the technical and non-technical communities with specific information about current cyber security issues, new vulnerability notification, potential impact assessment, and actions required to mitigate damage from an attack. US-CERT continues an active outreach effort that seeks to reach as many Americans as possible.

---

1 Update note: DHS has subsequently invested funds to augment the existing testing capability of the National Supervisory Control and Data Acquisition (SCADA) Testbed officially launched in May 2004 and run jointly by the Idaho National Environmental and Engineering Laboratory (INEEL) and Sandia. The National SCADA Testbed is aimed at SCADA systems only and aimed strictly at developing the capabilities to test energy sector systems. DHS's test center operates hand-in-hand with the SCADA Testbed, but the DHS effort is focused on the non-energy sectors and is trying to work with other existing private and public testbeds as to leverage their efforts and avoid duplication. In August 2004, the DHS Control Systems Security and Test Center (CSSTC) and the National SCADA Testbed were officially opened.

- The National Cyber Response Coordination Group

  The National Cyber Response Coordination Group (NCRCG), formerly known as the Cyber Interagency Incident Management Group (CIIMG), coordinates intra-governmental and public-private preparedness and operations to respond to and recover from cyber incidents and attacks and physical incidents and attacks that have significant cyber consequences. The group brings together officials from the Executive Office of the President, law enforcement, defense, intelligence, and other government agencies that maintain significant cyber security responsibilities and capabilities. In the event of an incident, NCRCG can provide a strategic picture of the impact to the information infrastructure and a coordinated response, due to its close association with others in private industry, academia, and international and local governments. The senior level membership of NCRCG helps ensure that during a significant national incident, the full range and weight of Federal capabilities will be deployed in a coordinated and effective fashion. The NCRCG meets monthly, and is developing cyber preparedness and response plans that will help it support the overarching mission of the DHS Interagency Incident Management Group. For example, the NCRCG has established communication protocols and coordination activities and conducted a tabletop exercise to identify gaps in performance.

To make security products more interoperable and to make response more efficient and effective, NCSD maintains and supports Common Vulnerability & Exposure (CVE), Common Malware Enumeration (CME), and Open Vulnerability Assessment Language (OVAL) tools. These tools and technologies are used extensively throughout the private sector and are generally accepted products that serve as the world's standards for addressing issues of vulnerabilities and malware. The initial phase of CVE-compatibility compliance has been completed for 165 of the 200 product or service offerings undergoing compatibility certification. Of the 165 that have completed phase 1, 34 have completed the second phase, the evaluation phase, and are fully CVE compliant.

US-CERT is also utilizing a number of technical tools to analyze potential vulnerabilities and weaknesses in cyber systems and improve overall situational awareness of the Internet. For example, NCSD has initiated Einstein, a pilot program designed to obtain flow data from federal government agencies' Internet access gateways and analyze the associated traffic patterns and behavior to provide US-CERT a better cyber security view and understanding across the federal government.

With regard to incident response, US-CERT also seeks to identify gaps in coordination, communication, and implementation of response policies and procedures during a cyber incident. In October 2003, DHS conducted the first ever national-level cyber exercise to baseline our capabilities for responding to national cyber attack. The exercise involved over 300 participants representing more than 50 organizations from across Federal, State, and local governments, as well as the private sector. Cyber attack simulation scenarios were developed to stress cyber interdependencies across America's critical infrastructures and baseline government agencies'

abilities to collaborate across the public and private sectors. Information gleaned from *Livewire* and similar exercises aimed at ensuring security of critical infrastructures is being used to improve our national incident response processes. While *Livewire* brought together a number of players for a large-scale event simulation, other exercises target specific areas or agency concerns. For example, in August, NCSD and the National Defense University (NDU) co-hosted a cyber security workshop to improve coordination among government agencies in response to a national level cyber attack and to specifically understand how the NCRCG will operate and respond. Additionally, NCSD conducted two regional exercises in New Orleans and Seattle to test specific regional and sectoral communication paths and responses to cyber attack.

The United States Secret Service's (USSS) Electronic Crimes Task Forces (ECTFs) have been running smaller regional and sector-specific tabletop exercises over the past eighteen months. These exercises are designed to help coordinate efforts in a targeted geographic area and are tailored to a specific regional infrastructure, such as the energy industry in Houston, TX, the high-technology industry in San Francisco, CA, and the banking and finance industry in Charlotte, NC.

Information Sharing and Awareness

To improve the Nation's cyber posture it is critical to increase the quality and amount of information sharing and awareness among the public and private sectors, including cyber security information, best practices, cyber incident information, and more. US-CERT and its communication mechanisms described above are key to our information sharing and awareness efforts, and we have established additional programs for similar outreach.

To enhance government coordination and response capabilities, NCSD launched a set of security forums: The Government Forum of Incident Response and Security Teams (GFIRST), a community of 40 government response teams responsible for securing government information technology systems. GFIRST works to understand and better handle computer security incidents and to encourage proactive and preventative security practices. The group has collaborated to provide technical analysis of ongoing cyber activities. This operation has improved the quality and quantity of information published via the NCAS, as well as specific information notices for the protection of government IT systems that are delivered to all Federal agencies. On four specific occasions, the group has worked together to identify previously unseen/unidentified cyber phenomena. Another forum is the Chief Information Security Officers Forum (CISO Forum), a venue for Federal IT security executives working for agency Chief Information Officers to facilitate education and cross-pollination of best ideas, peer-to-peer exchange, and access to subject-matter experts.

DHS also works with the States through the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Association of State Information Officer's (NASIO), and the National Governor's Association (NGA) to improve the cyber security of State and local governments across the Nation. These collaborative relationships help to facilitate coordination between Federal and State governments and among MS-ISAC members, to build awareness and education of cyber security issues, and to identify and facilitate the sharing of cyber security best practices, cyber incident information, and other relevant cyber information. Each of the States

receives unfettered access to the HSIN/US-CERT Portal, described above, and active collaboration and cooperation is underway between the NCSD and States to improve our national cyber security.

In addition, DHS co-sponsored the MS-ISAC's first Annual Conference in July 2004. DHS participated in the working groups during the conference and continues to participate with these groups as they execute their cyber plans.

DHS has also funded and launched a joint program between US-CERT and the MS-ISAC to improve cyber outreach and awareness among State and local government audiences. The primary focus of this initiative is the development of a series of national webcasts that examine cyber security issues. Webcasts were conducted in June, August, and October of this year, with a highly positive response and thousands of total participants. The October 19 webcast was held in conjunction with Cyber Security Month and participation was made available to home users in addition to Federal, State, and local government representatives.

Historically, companies and other entities have had concerns about the confidentiality of information shared with the Federal Government, either independently or through a mechanism like the ISACs. In response to these concerns, and recognizing that timely and broad participation in information sharing is necessary to provide accurate situational awareness of America's critical infrastructure, NCSD, in coordination with the Protected Critical Infrastructure Information (PCII) Program Office, is finalizing processes to expedite recurring "like" submissions of cyber-related critical infrastructure information (CII). Active members of the HSIN/US-CERT Portal can request permission to electronically send their CII information securely through the HSIN/US-CERT Portal directly to NCSD to decrease delivery time without compromising security. By teaming with the PCII Program Office, NCSD can help assure that members are able to submit CII information and that it gets to analysts without delay, thereby facilitating efforts to improve the overall situational awareness of the Internet and reduce the Nation's vulnerability to cyber security attacks.

Information sharing with the law enforcement and intelligence communities (LE/Intel) is crucial to making progress toward greater cyber security. NCSD engages directly with the LE/Intel communities in a number of ways, including a daily classified conference call between the National Security Agency, the Information Security Research Council (IRC), the Central Intelligence Agency, the DHS Office of Information Analysis, and the Joint Task Force Global Network Operations (JTF-GNO) to discuss cyber activity of note. This collaboration and interaction contributed directly to the National Intelligence Estimate of Cyber Threats to the U.S. Information Infrastructure (Cyber NIE). The resulting classified document issued in February, 2004 details actors (nation states, terrorist groups, organized criminal groups, hackers, etc.), capabilities, and, where known, associated intent. The NIE provides America's highest fused national threat assessment, and it is utilized throughout the defense, intelligence, law enforcement, and homeland security communities.

DHS has made significant strides in raising cyber security awareness and activity in international forums and bilateral discussions with our global partners. DHS has established a presence and is actively participating in interagency efforts in the Asia Pacific Economic Cooperation's (APEC)

Telecommunications Working Group, the Organization of American States (OAS), the Organization for Economic Cooperation and Development, and the Group of Eight (G-8). Each of these efforts strives to (1) establish the necessary national legal framework and enforcement capability; (2) establish national watch and warning capacity related to cyber incidents; (3) develop international information exchange capabilities; (4) develop public-private sector cooperation; and (5) raise awareness among stakeholders (governments, businesses, other organizations, and private citizens) of their roles and responsibilities for protecting the information infrastructure.

NCSD has also made progress on international cooperation and information sharing in two significant areas. NCSD has established a practice of regular (monthly or bi-monthly, depending on need) conference calls with our close allies of Australia, Canada, New Zealand, and the United Kingdom (with the U.S., often referred to as the "Five Eyes") to formulate a framework for ongoing policy and operational cooperation and collaboration. The framework currently functions through regular conference calls and is developing into a more formal, multilateral process. It will seek to continue and enhance current information sharing and incident response efforts among these Five Eyes allies, as well as foster collaboration in other international activities. The framework will also incorporate shared efforts on key strategic issues to address cyber security over the long term, including software assurance, research and development, attribution, control systems, and others.

NCSD is engaged in a multilateral effort to develop an international watch and warning framework that is designed to strengthen our National Cyber Security Response System through greater global situational awareness and cooperation. A key milestone toward such a framework was a multilateral conference co-hosted by the U.S. and Germany in Berlin, Germany in October 2004. The conference brought together policy, operational, and law enforcement representatives from fifteen (15) countries for interactive discussions of the vision, challenges, and existing models for watch and warning frameworks. The conference also included a facilitated discussion/tabletop exercise to baseline current international communication and incident response activities that helped determine the next steps toward an international watch and warning framework and enhance collaboration in preparation for, and response and recovery from, cyber incidents. As a result of the October conference, the participating countries expressed their intentions to:

a. Provide appropriate functional points-of-contact with national responsibility for cyber watch and incident response purposes;
b. Share appropriate and non-sensitive information for cyber watch purposes, which could include such aspects as:
    i. alerts and advisories
    ii. summary reports
    iii. ad hoc cyber security products such as white papers, best practices, etc., and
    iv. permit translation for publicly available documents
c. Share information on an on-going basis;
d. Communicate and coordinate response in case of a cyber incident with actual or potential global impact; and

e. Work toward more mature international cooperation and coordination on cyber information sharing and incident response.

NCSD will continue to take an active role in the post conference work in the remainder of 2004 and into 2005 and beyond.

Strategic Initiatives

In addition to the tactical initiatives that have helped to improve the state of cyber security in the near-term, it is critical to invest in more long-term strategic initiatives that will improve the underlying culture of software production, quality, and implementation. Specific areas of focus for these longer term activities include Software Assurance and Education and Training

Software Assurance

DHS is working closely with the private sector, academia, and other government agencies to improve software development processes in order to produce better quality and more secure software in support of mission assurance. For example, DHS is hosting and co-hosting various forums and workshops that include government, industry and academia that focus on topics such as developing curriculum standards and the improvement and evaluation of the Security Process Capability. As such, the NCSD has developed a software assurance plan that involves evaluating the software development lifecycle to mitigate risks and assure software integrity.

Discuss NCSD funding for DOD's NIAP review

In addition to specific software assurance efforts, NCSD is helping to fund other programs which address the development of more secure software and IT products. First, NCSD and DoD are funding a review of the National Information Assurance Partnership (NIAP), as called for in the Strategy, to determine the extent to which it adequately addresses security flaws. NIAP is a collaboration established in 1997 between the National Institute of Standards and Technology (NIST) and the National Security Agency to promote the development of sound security requirements for IT products and systems, as well as appropriate security evaluation metrics. The review is being implemented in three phases: 1) the collection of information regarding NIAP requirements, practices, and expectations (completed); 2) an analysis of the findings and the development of alternative options to increase NIAP's efficacy (underway); and 3) a detailed analysis of the feasibility of the options, with conclusions and recommendations for the future of NIAP (planned). Second, NCSD funded an economic study on Internet Protocol version 6 (IPv6) deployment through the Department of Commerce's IPv6-related task force. The task force is chaired by the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA). The study has been completed and will be used in the task force's forthcoming report on IPv6.

Education and Training

The Federal Government has undertaken several initiatives in partnership with research and academic communities to better educate and train future cyber security practitioners. DHS recently signed a Memorandum of Agreement (MOA) with the National Security Agency (NSA) to co-sponsor the NSA's Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program and to help expand it nationally to raise the prominence of the program and contribute to a well-prepared, growing cyber security workforce to support the public and private sectors. Currently there are 59 colleges and universities in 26 states and the District of Columbia designated as National Centers of Academic Excellence.

What are DHS's plans in the coming year in implementing the National Strategy for Cyber Security? Are there specific benchmarks you are using to evaluate progress?

Answer: As described above, NCSD has initiated a series of key activities to improve the cyber security posture of our Nation. Although much has been accomplished since the inception of NCSD last year, it is recognized that additional efforts are necessary to truly improve the Nation's ability to prepare for, and respond to cyber attack. As such, NCSD plans to improve the capabilities of our current initiatives and will implement a series of additional programs throughout the upcoming year. 2

All of DHS's efforts in cyber security aim to enhance the Nation's cyber security posture and, therefore, implement the five priorities outlined in the National Strategy to Secure Cyberspace. The nature of our cyber environment is consistently changing and rapidly evolving, making it difficult for both government and industry to set precise benchmarks and mechanisms to evaluate progress. Hence, we look to the successful implementation of our measurable programs and initiatives to evaluate our success. Implementation plans and related milestones in key cyber security areas include the following:

Priority I: A National Cyber Security Response System

Now that a robust national cyber security response system has been established through the US-CERT Operations Center, the HSIN/US-CERT Portal, the US-CERT Control Systems Center, the US-CERT public website, the National Cyber Alert System, and the National Cyber Response Coordination Group, DHS is focusing on making each of these elements more robust in order to build on our core capability and increase DHS's ability to prepare for, respond to, mitigate, and recover from cyber attack through public-private partnerships, greater analysis, improved situational awareness and communications efforts, and progress on our strategic initiatives.

The US-CERT digital control systems strategy incorporates five integrated goals to deal with issues and problems associated with control system security and includes working closely with

2 NCSD is currently addressing its designated milestones in the IP milestones and is establishing a strategic plan that will delineate future milestones and program funding.

industry owners and operators, vendors, and governmental agencies with jurisdiction over specific critical infrastructure sectors. The digital control systems strategy goals are to:

1. Facilitate the US-CERT's coordination of control system incident management, provide timely situational awareness information for control systems, and manage control system vulnerability and threat reduction activities. This coordination will create a capability to rapidly react to control system attacks and mitigate the vulnerabilities to high priority systems as quickly as possible. In addition, it will provide a focus for near-term activities aimed at securing the systems most critical to the Nation's infrastructure.

2. Create a DHS Control Systems Security and Test Center (CSSTC)that will provide a proactive environment for testing security, evaluating existing and next-generation equipment, working with control systems users and vendors to resolve identified vulnerabilities, and reducing vulnerabilities;

3. Bridge industry and governmental efforts through participation in various working groups with trade and professional organizations, standards development bodies and user conferences to build cooperative and trusted relationships, and enhance control systems security efforts;

4. Develop control systems security awareness and evaluative capabilities through training and outreach, and create a self-sustaining security culture within the control systems community; and

5. Develop a firm understanding of technology gaps in control systems security and make strategic recommendations as to the funding, development, and testing of next-generation secure control systems, and security products.

Exercises are one important way to identify gaps in cyber security readiness and evaluate progress over time. Future exercises will test cyber readiness in various geographic locations and critical infrastructure sectors across the Nation. In September and October 2004, regional exercises were held in Seattle, WA (Blue Cascades II) and New Orleans, LA (Purple Crescent II). Both exercises highlighted dependencies between cyber and physical infrastructures and interdependencies among critical infrastructures. Importantly, these exercises identified and tested the coordination and cooperation among Federal, State, and local governments with the private sector in the case of attacks (both cyber and physical) on the critical infrastructures in those regions of the U.S. In October 2004, the U.S. and Germany co-hosted a multilateral tabletop exercise in Berlin as part of a conference exploring the formation of an international watch and warning network to enhance global cyber watch efforts and incident response coordination.

DHS is playing an active role in development, facilitation and participation in a national exercise ("Top Officials"), to be held in the summer of 2005. This cabinet-level exercise will span a week and test not only response to attacks, but also continuity of government and continuity of operations, and response at the State, regional, and local levels, in areas including emergency

response, containment and mitigation of chemical, nuclear, and other attacks, etc.

The lessons learned from these and other exercises will form the backdrop for an NCSD-sponsored National Cyber Exercise planned for fall 2005 that will: (1) sensitize a diverse constituency of private and public-sector decision-makers to a variety of potential cyber threats including strategic attack; (2) familiarize this constituency with DHS' concept of a national cyber response system and the importance of their role in it; (3) practice effective collaborative response to a variety of cyber attack scenarios, including crisis decision-making; (4) provide an environment for evaluation of interagency and cross-sector business processes reliant on information infrastructure; (5) measure the progress of ongoing U.S. efforts to defend against and respond to attacks; (6) foster improved information sharing among government agencies and between government and industry; and (7) practice roles and responsibilities of government agencies and industry in cyber incident response.

Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program

Comprehensive vulnerability assessment is a necessary aspect of overall homeland security. As part of the Critical Infrastructure Protection initiative mandated under Homeland Security Presidential Directive 7 (HSPD-7) issued by President Bush on December 17, 2003, the Department of Homeland Security is coordinating vulnerability assessments of critical infrastructures in cooperation with the designated sector-specific agencies. Under HSPD-7, sector-specific agencies have responsibility to identify critical assets, develop methodologies to assess vulnerabilities, and map those vulnerabilities to critical assets in a risk assessment analysis. DHS is responsible for the correlation, analysis, and trending of the information provided by those agencies. DHS is the information technology (IT) sector-specific lead agency, and NCSD has been delegated the specific responsibility for the IT Sector. As such, NCSD is charged with identifying the critical assets and related vulnerabilities in the IT sector.

In addition, DHS is producing a comprehensive inventory of cyber security assessment, remediation, and mitigation activities conducted within and across critical infrastructure sectors. NCSD is also contributing cyber security guidance to assist critical infrastructure sector-specific agencies in the development of their CIP plans as the lead subject matter expert responsible for the cyber review of all of the sector specific plans. NCSD will work with each sector-specific agency to assist them as they operationalize their plans. NCSD is also supporting the Office of Management and Budget (OMB) in their review of Federal agency cyber CIP plans.

After the initial assessment and determination of vulnerabilities by all sector-specific agencies, a remediation plan will be developed within each sector-specific agency to address the vulnerabilities. NCSD's ongoing cyber threat and vulnerability programs facilitate the effort to complete and maintain a critical cyber asset inventory; implement and expand standard methodologies to perform threat, risk, and vulnerability assessments; develop and maintain an interdependency analysis capability to systematically understand the relationships between cyber and physical assets; and identify priority protective measures to mitigate vulnerabilities.

To understand cyber risk, it is critical that both threats and vulnerabilities be examined. As such, NCSD is actively coordinating with the intelligence community to review, understand, and

quantify the cyber threats facing our Nation. Once finished, a complete risk assessment will be conducted that integrates the findings of these efforts.

Priority III: A National Cyberspace Security Awareness and Training Program

DHS has signed an MOA with the National Science Foundation (NSF) to cosponsor and improve the Scholarship for Service (SFS) program, also known as the Cyber Corps program. The SFS program provides scholarship grant money to selected CAEIAEs and universities with programs of a similar caliber, to fund the final two years of student bachelors, masters, or doctoral study in information assurance. The program is expected to produce 200-300 highly trained professionals per year by FY04, and 400 by FY05. Students who receive scholarships agree to work for a Federal agency for a period of two years.

In addition, although over ninety cyber security-related certifications currently exist, no cohesive and consistent job or skill standard has guided certification development. In order to establish greater consistency and reliability among certifications, and ensure that they measure competence that translates to job performance, DHS and DoD have partnered to create a national-level job task analysis (JTA). The JTA will first be conducted within DoD, and subsequently expanded to the Federal level by coordinating with the Federal CIO Council's Subcommittee on Workforce and Human Capital for Information Technology. As the Federal JTA is getting established, NCSD will engage with private sector stakeholders to integrate private sector data and thought leadership into the program. The end product will be a national-level JTA that (1) describes skill standards for information assurance for both the public and private sectors; (2) provides a baseline that will allow industry certifications to be mapped to specific jobs; and (3) clarifies the job skills upon which to build future certifications.

Priority IV: Securing Government's Cyberspace

DHS/NCSD has engaged the Chief Information Security Officers (CISO) Forum to undertake an examination of agencies' needs, as well as the current state and future development of patch technology. One CISO Forum working group is studying current patch technology and identifying agencies' common needs, while another is considering how the patch management industry can assist in responding to sudden and potentially damaging exploitation of vulnerable software. The working groups are drafting best practices for agency CIOs to consider.

We are currently in the process of expanding the Einstein pilot program's capability across the federal government. By increasing situational awareness through information gleaned from participating Federal government agencies, the US-CERT will be able to analyze indications and warnings of potential cyber attacks or threats. Additionally, this program will help agencies identify configuration problems, unauthorized/unnecessary network traffic, network backdoors, and routing anomalies, among other anomalous activity.

Priority V: National Security and International Cyberspace Security Cooperation

NCSD's international program includes active participation in various bilateral, regional, and multilateral cyber security efforts. As a result of work accomplished to date, some of NCSD's plans include continuing efforts to:

- Formalize collaboration framework with Five Eyes countries;
- Implement results of U.S.-Germany sponsored multilateral cyber security conference in Berlin (October 2004) including information sharing mechanisms and work toward more mature international watch, warning, and incident response framework;
- Further the U.S.-India Cyber Security Forum efforts with increased cooperation between US-CERT and CERT-India (CERT-In), including information sharing efforts and a planned joint workshop in New Delhi in 2005;
- Further the U.S.-Mexico Framework for Critical Infrastructure Protection through new efforts in the recently established Cyber Security Working Group;
- Further the U.S.-Canada Framework for Critical Infrastructure Protection through new efforts in the recently established Cyber Security Working Group;
- Further established bilateral efforts with Australia and the United Kingdom as well and recently established bilateral discussions with Italy, Hungary, and others.
- Regularize the collaborative and information sharing efforts of the so-called "Five Eyes" group (U.S., Australia, Canada, New Zealand, and the United Kingdom);
- Work with the Organization of American States (OAS) to create a regionally-based information sharing framework;
- Work within the Asia Pacific Economic Cooperation (APEC) to incorporate the work of regional computer security incident response teams into the work program of the APEC Telecommunications Working Group (APEC TEL);
- Work with the Organisation of Economic Cooperation and Development (OECD) to implement the OECD's *Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security.*

The MyDoom worm that was reported in many papers last week, targeted a Utah company. Could you explain the role of DHS and the National Cyber Alert System (announced Jan 28) played in handling this cyber incident? How did DHS discover the worm? What did it do once it got the information? Did it share the information with anyone? Did it coordinate with software vendors? Did it contact the Utah company directly? Did the National Cyber Alert System work properly? Was the federal government able to protect its systems? Could you explain the role of DHS and the National Cyber Alert System (announced Jan 28) played in handling this cyber incident?

Answer:

DHS' NCSD coordinated the combined public-private response to the MyDoom virus. NCSD disseminated both a technical and non-technical alert to its constituents through the NCAS. The alert provided a detailed analysis of the incident, specific

recommendations for mitigating infection, and a series of response activities that infected users could implement to quickly recover, thereby limiting downtime and disruption.

How did DHS discover the worm?

NCSD first became aware of the existence of the MyDoom virus through various public and private sources, including HSIN/US-CERT Portal members, on January 26, 2004.

What did it do once it got the information?

NCSD representatives immediately began communicating and coordinating with partner organizations, law enforcement, and the intelligence community to mitigate the effects of the virus and its variants. The members of the NCRCG (formerly known as the CIIMG) were contacted and notified of the situation and the possibility of that group being convened regarding this virus. Physical and communications contingencies for a meeting of the NCRCG were established.

Did it share the information with anyone?

Yes. The US-CERT shared the available information about the MyDoom virus with over a half a million people through the National Cyber Alert System, the HSIN/US-CERT Portal, and the US-CERT public website.

Did it coordinate with software vendors?

Yes. Representatives from US-CERT coordinated, either directly or through partners, with the affected vendors and representatives of the antivirus community.

Did it contact the Utah company directly?

Yes. US-CERT representatives initially reached out to the SCO Group. NCSD law enforcement representatives maintained an open channel of communications with law enforcement representatives working the investigation in Utah throughout the incident.

Did the National Cyber Alert System work properly?

Yes. Due to the initial impact of the MyDoom virus, NCAS was launched days earlier than planned and issued the first of its alerts on the MyDoom virus. Standard alert SA04-028 and technical alert TA04-028 were released. While not flawless in its initial release, the first alerts proved successful in reaching a large constituency in a very short period of time. Since its debut, the NCAS has matured and is currently capable of reaching over 250,000 subscribers.

Was the federal government able to protect its systems?

The agencies of the Federal Government were not directly impacted due to the nature of

the malicious code. The .gov and .mil domains were explicitly removed from the list of possible targets within the virus code. However, the experience of the MyDoom incident continues to inform efforts to improve the security of Federal Government systems.

4. The National Cyber Alert System is designed as an information sharing tool. How does it work? Does it do anything more than issue general alerts? Does it provide targeted information to specific critical infrastructure sectors? Is it secure? How do people use the system to provide information to the government? How does the Critical Infrastructure Information Act (including the Freedom of Information Act (FOIA) provisions) work with this system?

Answer: The lynch pin to preventing the spread of computer viruses and worm outbreaks is a robust and mutually beneficial relationship with the private sector. Cyber security is often a reactive process because the initiative rests with hackers and malicious agents. Developing and maintaining a partnership with the private sector is therefore a crucial means to both responding quickly to emerging threats and taking proactive measures to forefend against potential threats. The DHS/US-CERT Partner Program is composed of members that recognize their responsibility to their organizations and the nation to improve the current and future state of cyber security. Members collectively and individually realize the need to take action and abide by principles and practices that are appropriate as critical infrastructure operators, communities of interest, vulnerability researchers, educators, and software vendors. The Partner Program consists of participants from various sectors of the cyber community who must agree to meet certain criteria in order to achieve the designation of DHS/US-CERT partner. These criteria are designed with the aim of preventing occurrences such as the spread of computer viruses and worms and other malicious activities. The Protected Critical Infrastructure Information Program Office is working with the DHS/US-CERT to develop procedures to offer protection under the Critical Infrastructure Information (CII) Act to private sector entities who wish to voluntarily submit CII material to the federal government.

Another important tool for the prevention of worms and viruses is the National Cyber Alert System. Americans are exhibiting a keen interest in the alert system. On day one of the National Cyber Alert System launch, we had more than one million hits to the US-CERT website. Today, more than 250,000 direct subscribers are receiving National Cyber Alerts to enhance their cyber security. Through the alert systems, Americans are able to receive information that is accurate and actionable. It is our goal to inform the public about the true nature of a given incident, what the facts are, and what steps they can and should take to address the problem. The offerings of the National Cyber Alert System provide that kind of information. To date, we have issued seven security tips, six security bulletins, ten technical alerts, and six non-technical cyber alerts in response to cyber security incidents through the National Cyber Alert System. We strive to make sure the information provided is understandable to all computer users, technical and non-technical, and reflect the broad usage of the Internet in today's society. As we increase our outreach, the National Cyber Alert System is investigating other vehicles to distribute information to as many Americans as possible.

Post-Hearing Questions for the Record
Submitted to the Honorable Tom Ridge
From Senator Daniel Akaka

"The Department of Homeland Security's Budget Submission for Fiscal Year 2005"

February 9, 2004

Human Resources System

1. At the hearing you testified that funding for the Department's recruitment and retention efforts, including the use of student loan repayment, is not included in the amount requested for the new human resource system but is available in the FY05 DHS budget request. Please clarify for the record where funding for student loan repayment is located in the budget, and how much funding the Department plans to use in FY05 for its student loan repayment program. Please also provide information on the Department's student loan repayment program, including the criteria for using this authority (i.e., whether student loan repayment is authorized for specific positions, based on the financial need of employee, is used for hard to fill or critical need positions, etc.).

Answer: Funding for the student loan repayment program, as well as the other recruitment and retention incentives, would be included in salaries and expenses. The standards for this program are set by the Office of Personnel Management (5 CFR 537). The Department has prepared a "model plan" for implementing this program as part of its overall policies on recruitment and retention – the criteria for the program are therefore linked to issues associated with filling positions and/or retaining current employees in mission critical functions. To date, none of the components have implemented this program, although several have established policies or are in the process of drafting procedures as required by the OPM guidance.

2. You said at the hearing that proposed regulations for the Department's new human resources system will be published soon. The FY05 budget request includes $2.5 million for a pay-for-performance system, $42 million for the design and implementation of a pay-for-performance system and for the administration and staffing of the new labor management and appeal process, $31 million for training employees to implement a new pay-for-performance system, and $27 million for program management. Assuming the proposed regulations are implemented as drafted, what process did you rely on to determine that the FY05 budget request was sufficient to implement the system in each of these areas? Did you rely on the advice of a contractor in making this determination? If so, who was the contractor and what information was provided?

Answer: The budget request for FY05 was developed by the Chief Human Capital Office, Department of Homeland Security, without advice of a contractor. The estimates are based on known costs for developing performance management systems and designing training programs and beginning to roll out training for the managers, supervisors and rank and file employees. Program management costs were estimated based on experiences in other Departments and

agencies in designing and managing major human resource initiatives. The pay for performance estimate is based on the approximate expenditures needed to create a performance pool equal to within grade increase, quality step increases, and career promotions in the workforce.

3. The 2004 Defense Authorization Act included language establishing a Human Capital Performance Fund. The 2005 budget requests $300 million for the program. As the Department has the authority to set up a pay-for-performance system, do you anticipate the Department applying to Office of Personnel Management (OPM) to use these funds? If so, how much do you anticipate needing?

Answer: The Department has not determined whether it will apply to OPM for the use of funds from the Human Capital Performance Fund.

4. The Department has requested $31 million for training managers for the implementation of a new pay-for-performance system. Training is essential to having a high quality workforce, for dealing with poor performing employees, to being an effective manager, and for general professional development. In addition to the $31 million requested for the pay-for-performance system, how much money is the Department requesting for other training activities? Please provide a description of these training activities and the amounts requested.

Answer: The Department received $36 million to fund design and deployment of the Department's new human resources management system, MAX^{HR}. Of this amount, the Department is proposing to spend an estimated $8-10 million dollars on training activities associated with deployment of the new system, including training of Departmental executives, managers, employees and HR professionals. In addition to the funding that has been allocated as a part of our MAX^{HR} initiative, the Under Secretary for Management, Chief Human Capital Office has proposed to invest an additional $1.249 million in bolstering Department wide Leadership Development activities in FY 2005. Examples of priority leadership development initiatives would include:

- $ 60k for a Secretary's Executive Conference
- $950k for Senior Executive Service Candidate Development Program
- $239k for DHS Headquarters Executives, Managers, and Supervisors (e.g., $25k for SES Forum Series; $104k for participation in coursework at the Treasury Executive Institute; $110K for individual executive and management development)

Funding of Other Offices in the Management Directorate

1. The budget requests $103 million for the Office of the Secretary and Executive Management. How much of this amount is allocated to the Privacy Officer and the Office of Civil Liberties and Civil Rights? Is this an increase or decrease from last year? What is the rationale for the requested change?

Answer: The FY 2005 enacted amount for the Privacy Office totals $3,774,408, representing an increase of $3,006,963 over the FY 2004 enacted level of $767,445. The requested resources will support an increase of 8 FTE over the FY 2004 FTE level of 4. In addition, funding is

requested for FOIA contract support and the development of a FOIA/ records management system.

The FY 2005 enacted amount for the Office of Civil Rights and Civil Liberties totals $13,000,000, representing an increase of $49,859 over the FY 2004 enacted level of $12,950,141, for pay and non-pay inflationary adjustments.

Non-Homeland Security Mission Performance

1. The Department's budget contains information on the amount of money spent on homeland security and non-homeland security missions. However, the budget does not identify which missions fall into which category. Please provide for the record a breakdown of the homeland security and non-homeland security missions. Please also describe how these determinations were made, and whether these determinations change over time or are re-evaluated on an annual basis.

Answer: Based on the definition provided by OMB, homeland security activities focus on combating and protecting against terrorism that occurs within the United States and its territories (this includes Critical Infrastructure Protection (CIP) and Continuity of Operations (COOP) data), or outside of the United States and its territories if they support domestically-based systems or activities (e.g., visa processing or pre-screening high-risk cargo at overseas ports). Such activities include efforts to detect, deter, protect against, and, if needed, respond to terrorist attacks. Generally, anything that does not fall into this category is considered a non-homeland security activity. The methodology used to divide resources between homeland security and non-homeland security is described below by component.

FY 2005 Estimating Methodology:

Departmental Operations
-- Homeland security activities include headquarters critical infrastructure protection (physical security, cyber security) and 60% of the remaining non-programmatic budget. The non-homeland security resources include identified non-homeland security activities (such as HR system, NAC renovations, and the Office of Immigration Statistics), plus the left over 40% of the non-programmatic budget.

CT Fund
-- The CT Fund is 100% homeland security.

Department-wide Technology
-- Homeland security activities include the Wireless program, Watch-list Integration, and I/T Evaluation program.

Office for Domestic Preparedness
--Funding for State and Local Programs is 100% homeland security.

--Funding for Firefighter Assistance Grants is 100% homeland security in FY 2005. Previously, funding was 100% non-homeland.
-- In FY 2005, the firefighter grant resources have been proposed to be distributed with priority to enhancing terrorism preparedness.

U.S. Immigration Services
--Immigration Services funding is 100% non-homeland security.

Office of the Inspector General
--Funding for the Office of the Inspector General is 100% non-homeland security.

U.S. Secret Service
--Homeland security activities include 100% of Protective Operations funding and 75% of Investigative Operations funding within the Salaries & Expenses account. The Acquisition account is split 87% homeland security and 13% non-homeland security.
--The mandatory retirement is 100% non-homeland security.

Border and Transportation Security Directorate
--U/S BTS is 100% non-homeland security funding.
--US-VISIT is 100% homeland security.

U.S. Customs & Border Protection
--As a general rule, 100% of legacy INS functions are homeland security, while only 63% of legacy Customs functions are homeland security.
--In the Salaries & Expenses account you deduct the border patrol and attribute those resources to homeland security. The remaining dollars are split 63% homeland to 37% non-homeland.
--The Automation Modernization account is divided 50/50 across all programs.
--CBP Construction is 100% homeland security funding because it funds border station construction.

U.S. Immigration & Customs Enforcement
--As a general rule, 100% of legacy INS functions are homeland security, while only 63% of legacy Customs functions are homeland security.
--The Salaries & Expenses, Automation Modernization, and Air & Marine accounts deduct legacy INS program, and the remaining Customs functions are split 63% homeland to 37% non-homeland.
--The ICE Construction, Federal Protective Service and Federal Air Marshals accounts are 100% homeland security.

Transportation Security Administration
--Resources for the transportation security administration are considered 100% homeland security.
Federal Law Enforcement Training Center
--Homeland security activities only include training funding.
--Management and oversight funding is considered non-homeland security funding.

U.S. Coast Guard
--The Homeland Security Act designated five of the Coast Guard's missions as Homeland Security activities: drug interdiction; migrant interdiction; port, waterway, and coastal security; protection of the Exclusive Economic Zone (EEZ); and defense readiness. Coast Guard uses their cost model to determine the level of resources dedicated to each of these missions.
--The non-homeland security mission areas are: search & rescue; marine safety; aids to navigation; ice operations; marine environmental protection; living marine resources.

Emergency Preparedness & Response
--Resources for the following accounts are considered 100% non-homeland security:
U/S EP&R
Disaster Relief Fund
Mitigation Grants
Flood Insurance Fund
Radiological Emergency Preparedness
Flood Map Modernization
Disaster Assistance Direct Loans

2. The FY05 budget request cuts the proportion of funding in the DHS budget dedicated to traditional missions. How will funding cuts to non-homeland security missions impact the Department's ability to fulfill its traditional missions?

Answer: In the overall budget from FY04 to FY05 there is a 4% fluctuation in the proportion of funding dedicated to traditional missions of the Department. Rather than cutting the funding for non-homeland missions, the FY05 budget realigns and refocuses how the resources are utilized. Despite some resources being re-classified, the nature of both the homeland security and the non-homeland security missions are still being fulfilled.

Homeland Security Grant Programs

1. Some homeland security responsibilities in the Department received funding cuts. These included programs for disaster mitigation, emergency management planning, first responder training, and port security. Most of the cuts were in grant programs. Could you please explain for the record why this was the case?

Answer: The Fiscal Year 2005 budget provides $3.6 billion for the Office for Domestic Preparedness, which has the primary responsibility within the Federal government to build and sustain the preparedness of the United States to reduce vulnerabilities, prevent, respond to, and recover from acts of terrorism. The FY 2005 budget, which is $3 million more than the FY 2004 budget, is a significant commitment to providing funds to our nation's emergency prevention and response community, and continues the Administration's effort to secure the nation from acts of terrorism.
The budget includes a doubling of funds for the Urban Areas Security Initiative (UASI) and will effectively shift funds away from arbitrary formulas to allocations based more on threat assessments. This will allow the Department to reinvigorate its commitment to providing

homeland security funds based on terrorism risks, threats, and vulnerabilities. Included in the budget is $400 million for the continuation of the law enforcement terrorism prevention grant program, which focuses more funds on prevention and deterrence activities. This is an increase of nearly $3 million compared to the FY 2004 budget. Finally, the budget includes $715 million for continuation of the Assistance to Firefighters Grant Program. This is consistent with the Administration's FY 2004 request and provides significant funds for the continuation of this highly successfully and critically important program.

2. States rely on the Department of Homeland Security (DHS) to provide guidance on the actions needed to prepare for acts of terrorism. This requires strong communication and guidance which allows states maximum flexibility to address homeland security needs. One of the ways the Department accomplishes this is through technical assistance for homeland security planning. The budget request cuts technical assistance funding by 66 percent, from $30 million to $10 million. Why was technical assistance cut and how will the Department now ensure appropriate guidance for emergency planning?

Answer: The Fiscal Year 2005 enacted amount for the Office for Domestic Preparedness includes $30 million for technical assistance, which is the same as the Fiscal Year 2004 enacted level. This reflects the recognition of a continuing major funding commitment to assist the States with developing their congressionally-mandated homeland security strategic plans. At this time, ODP has received and reviewed all State strategic plans.

3. The President's Budget request cuts Emergency Management Performance Grants by $9 million and proposes a 25 percent cap on funding used for personnel costs from the grant. This could cause a heavy strain for states. According to the National Emergency Management Agency (NEMA), restricting the amount of grant funds used for personnel will devastate state and local emergency management programs and the nation's emergency response system. States already experience emergency management personnel shortfalls. According to NEMA, states could lose up to 60 percent of their emergency management staff, should this cap be imposed. Could you please explain for the record, why DHS is imposing this cap and how the EMPG funding cut and personnel cap will impact national preparedness?

Answer: The President's Fiscal Year (FY) 2005 provides $170 million for the Emergency Management Performance Grants (EMPG) program, which is a $20 million increase over the FY 2004 requested level. In fact, the FY 2005 requested level is the largest amount ever requested for this program, which clearly demonstrates the Administration's support for this important program. By limiting the amount of the award that can go to salaries, we are increasing the amount of funds available for planning, training and exercises. Furthermore, the budget request does allow for salaries, but shifts the emphasis to federal support for planning while properly aligning responsibility for staffing and salaries with the states and local governments. The Administration firmly believes that homeland security is not solely a responsibility of the Federal government, but one of shared responsibilities and collaborative efforts among Federal, state, and local partners.

U.S. – Visit

During the hearing you testified that DHS is in conversation with the European Union to establish standards for biometric identification. Could you please provide for the record when you expect to reach an agreement on these standards?

Answer: The international standards for biometric identification were recently finalized. The International Civil Aviation Organization (ICAO), the organization responsible for defining international standards for biometrics as applied to passports and border crossing applications, approved and finalized these standards during a meeting at ICAO headquarters in Montreal the week of 17 May 2004. A follow-up meeting of the e-Passports ICAO/New Technology Working Group (NTWG) was held in London on 17 June 2004 to clarify specifications to ensure that global interoperability can be achieved. Further interoperability testing of prototype passports, chips and readers was conducted in West Virginia, US, in July 2004, hosted by DHS. Individuals from 18 nations participated in the testing. Basic interoperability of chips and readers was achieved, but technical issues remain. Another round of testing was conducted in Sydney, Australia in August 2004. The United States will host a mock port of entry test in October to test chips and readers in an operational environment.

Port Security

1. As you know, the President's budget request contains no funds to meet port security requirements. The Maritime Transportation Security Act authorizes federal support for port security and Congress has allocated $493 million in port security grants since 9-11. Could you please provide for the record an explanation of why port security grants are not funded in the FY05 budget request, how much funding DHS will make available for port security assessments, and where this funding will come from?

Answer: Port Security Grants will be funded in FY 05 by security service fees authorized from "Title 49 U.S.C. 44940 credited to this appropriation as offsetting collections and used for security services authorized by that section". (DHS Congressional Budget Justification, Page TSA-62) For FY 2005, Congress has appropriated $150 million for port security grants.

In the final MTSA regulations, the Coast Guard estimated the industry cost for implementing Section 102 of the MTSA security requirements as approximately $1.5 billion in the first year, and $7.3 billion over the next 10 years. The port security grants to date have provided approximately $500 million.

First Responder Interoperability

1. SAFECOM, which provides public safety agencies the guidance to achieve interoperable communications, does not have a specific funding level in the budget. Please explain why there no specific funding level for SAFECOM in the budget and how much funding DHS plans to devote to SAFECOM in FY05?

The SAFECOM program, within DHS's Science and Technology Directorate, is the umbrella program within the federal government charged with coordinating the efforts of local, tribal, state, and federal public safety agencies to improve public safety response through more effective, and efficient interoperable wireless communications. SAFECOM is an E-Government interagency program. As an E-Gov initiative, SAFECOM has been funded by partner agencies. The partner agencies include the Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Interior, and Justice. The result is that no specific funding request is reflected in the DHS budget, although DHS indeed supports SAFECOM's efforts to coordinate and streamline all federal public safety communications and interoperability initiatives. SAFECOM has been allocated $26.023 million in funding for FY 2004 and anticipates a budget of $22.105 million for FY 2005.

Terrorist Screening Center

1. According to Terrorist Screening Center (TSC) officials, Freedom of Information Act and record retention issues will be addressed by an Ombudsman. When will the TSC establish an Ombudsman to ensure that FOIA and records retention issues are properly addressed? As a member of the TSC, could you please provide for the record how DHS will work to ensure that TSC records are properly managed and that persons incorrectly included in TSC databases are removed?

Answer: This question should be referred to the Terrorist Screening Center.

2. The only declassified data elements that the TSC can share with state and local officials is a person's name, date of birth, passport number and country of origin. TSC will offer leading questions to law enforcement officials in order to identify a suspect. How does the TSC plan to identify reliably suspected terrorists if only unclassified information may be shared with state and local law enforcement officials? Should there be a way to share classified information with properly cleared state and local officials?

Answer: This question should be referred to the Terrorist Screening Center.

Geospatial Information Database

1. As you know, I have long had an interest in using geospatial information to enhance our response to disasters. During the hearing you agreed to provide me the Department's strategy for acquiring such a capability and the time frame for its development.

Answer: Please see the answer to question 2 below.

2. In addition, what is Department's strategy and plan is for developing any necessary prototype databases of national geospatial information which would be used in both counter-terrorism efforts, and disaster response?

Answer : The Department does recognize the importance of geospatial information and location based intelligence, and the value of such information to the Mission of Homeland Security. We recognize the cross cutting nature of geospatial information and through our efforts to document the current state of operations in the department, see a significant amount of activity in this area. In response to this reality, the Department has taken steps to develop an enterprise strategic approach to providing geospatial solutions to the planners and decision makers, both within the Department, and for the key stakeholders with whom the Department will work to protect the homeland.

The department is initiating a program office to work specifically on developing a strategic geospatial solution. To date, we have developed a draft strategic plan and forward-looking enterprise architecture for geospatial solutions. Two of the basic tenets of this plan are communication and interoperability. The key to success in the geospatial arena is interoperability. The strategy we are developing is built on an interoperable framework, or architecture, enabling maximum use and re-purposing of geospatial assets. Following the good guidance of the President and the Legislature, we are developing the strategic approach which will allow direct engagement of other Federal partners and our State and Local partners to develop a system in which interoperability becomes a reality, information sharing is enabled, redundancies are reduced, and cross-purposing of assets is enabled. This will open the door for communication between the Department and its stakeholders on a new level of effectiveness, and will maximize the contribution to the mission of securing the homeland.

Key federal partners in this effort include the Department of Interior, through the U.S. Geological Survey, and the Department of Defense, through the National Geospatial Intelligence Agency. Initial architectural implementations of combined geospatial capabilities, supporting homeland security, will be undertaken in FY04. Operations currently in place will continue, and the initial transition to the enterprise strategic approach will begin in FY04 and continue through FY05. Placement of assets within this enterprise geospatial architecture, including the geospatial data assets to which your question refers will be distributed. Homeland Security needs for geospatial data are great, and represent a significant capital asset. The distributed model will enable stakeholders to use the considerable existing assets in the geospatial community, and will allow access for those stakeholders to assets acquired by the Department. This enables maximum access for all Homeland Security stakeholders, in a two-way communication chain, to

all geospatial data and information sources, and will be implemented with multiple levels of security. This approach will allow sharing of information and assets, as well as protection of sensitive information.

Thank you for the opportunity to discuss this important issue and I look forward to working together in the future to assure the Department works cooperatively with the key stakeholders, including your constituency, to implement an effective and collaborative approach to information sharing and communication in support of securing the homeland.

Bureau of Immigration and Customs Enforcement (BICE)

The budget calls for $226 million for the Department's information technology (IT) equipment. I understand that the Bureau of immigration and Customs Enforcement (BICE) has had some trouble consolidating its IT systems to perform such functions as travel, firearm accounting, and payroll. What percentage of this amount, if any, will be used by BICE to streamline and consolidate its IT systems? What additional funding, if any, will be used by BICE for this purpose?

ICE currently maintains its firearms in the legacy system, Asset Management Information System (AMIS). Firearms accountability will be integrated with the Department-wide solution under the eMerge2 domain. Additionally, we will continue to explore and implement, where possible, the use of radio frequency identification to track and account for our weapons.

Science and Technology

1. The Department's budget proposes a cut of $38.8 million in the university and fellowship programs within the Science and Technology Directorate. When questioned about this decrease at the hearing, you responded that the Department wanted to maintain the program in FY 2005 and grow it later. Please explain how the fellowship program will be 'maintained' with a decrease of $38.8 million. As such programs contribute to the Department's efforts to recruit individuals possessing science and technological skills important to protecting the nation, please provide a detailed description of the Department's overall recruitment and retention programs as well as the funding requested for these programs for FY05.

Answer: Maintaining a cadre of talented scientists and engineers and investing in our future scientific workforce is essential to the success of the Department of Homeland Security (DHS). The Department's University Programs within the Science and Technology (S&T) Directorate funds both fellowships and scholarships, and the establishment of University Centers of Excellence. These activities contribute to the Department's efforts to recruit individuals possessing science and technological skills important to protecting the nation. The Department intends to sustain the current number of DHS scholars and fellows. Scholars and fellows are selected in disciplines of importance to DHS, including the social sciences. Presently, DHS is formalizing its Human Resources personnel system. Following adoption of this system, the S&T Directorate will work with the Human Capital Office to determine appropriate recruitment and retention strategies specific to the needs of the S&T Directorate and DHS. The Department did

not make any specific FY 2005 funding requests for its overall recruitment and retention programs pending completion of the Human Resources personnel system.

Post-Hearing Questions for the Record
Submitted to the Honorable Tom Ridge
From Senator Frank Lautenberg

"The Department of Homeland Security's Budget Submission for Fiscal Year 2005"

February 9, 2004

(1) The Administration has adopted a narrow interpretation of the Brady gun control law, which has thwarted the efforts of U.S. law enforcement and counterterrorism agencies to track the illicit activities of suspected terrorists on the FBI's Violent Gangs and Terrorist Organization Files (VGTOF).

Do you believe that we should, in any way, interpret our federal gun control laws to prohibit federal authorities from sharing critical information with law enforcement about known terrorist suspects who purchase firearms in the United States?

Answer This question should be referred to the FBI or TSC.

(2) Would you support legislation that permits the National Instant Criminal Background Check System (NICS) to provide FBI field offices or other law enforcement and counterterrorist agencies with critical information (such as the specific location of the sale and the type of weapon purchased) related to the purchase of firearms by suspected terrorists in VGTOF?

Answer: This question should be referred to the FBI or TSC.

(3) Despite consensus opinion in Washington that police, fire and other local personnel are on the frontlines in the war on terrorism, the administration cut the first response budget this year– from $4.2 billion in 2004 to $3.5 billion for 2005. I am shocked and disappointed that the president's budget in its entirety cuts more than 15 percent of the overall funding for first responders, decreases by 43 percent cut the first responder training, and significantly slashes local fire and law enforcement grants. The FIRE Act program received a 33 percent reduction, and the SAFER program did not receive any new funding.

What can say to our brave public servants about the decrease in funds this year for their police, fire and other response work?

Answer: It is simply inaccurate to portray the President's budget request as cutting 15 percent of overall funding for first responders. The President's budget request included a $ 3.3 million increase in the overall budget for the Office for Domestic Preparedness, the Department's principal agency responsible for working with our Nation's emergency prevention and response community, and a 10 percent increase in funding for DHS as a whole.

Congress recently passed the FY 2005 DHS Appropriations Act, which continues the strong commitment to our Nation's emergency prevention and response community by providing nearly

$4 billion to the Department's Office of State and Local Government Coordination and Preparedness, Office for Domestic Preparedness. Included in the final appropriations act (P.L 108-334), which the President signed on October 18, 2004, is $1.1 billion for the State Homeland Security Grant Program, $400 million for the Law Enforcement Terrorism Prevention Program, $180 million for the Emergency Management Performance Grant Program, $885 million for the Urban Areas Security Initiative, $150 million for port security, $150 million for rail and transit security, and $715 million for continuation of the Assistance to Firefighters Grant Program.

(4) Will DHS be initiating any new grant programs for municipalities during FY 2005?

Answer: In FY 2005, the Department of Homeland Security's Office of State and Local Government Coordination and Preparedness will administer two new programs that could benefit local communities and municipalities: a technology transfer program, which will be a direct delivery program that focuses on the technology needs particularly of smaller, rural jurisdictions, and a firefighter personnel hiring program. Congress included as part of the Department's FY 2005 Appropriations Act (P.L. 108-334) $50 million to develop a technology transfer program to "assist smaller communities in acquiring and using commercially available technologies to prevent, deter, and respond to terrorist attacks, as identified in state homeland security strategies." SLGCP, which will administer the program, is currently developing the procedures and guidelines for this new program. Also, Congress provided $65 million in the FY 2005 DHS Appropriations Act to administer a firefighter staffing program that is authorized by Section 34 of the Federal Fire Prevention and Control Act of 1974. This program is also known as the Staffing for Adequate Fire & Emergency Response Firefighter's (SAFER) program. SLGCP is currently developing the procedures and guidelines that will govern this program.

Post-Hearing Questions for the Record
Submitted to the Honorable Tom Ridge
From Senator Joseph Lieberman

"The Department of Homeland Security's Budget Submission for Fiscal Year 2005"

February 9, 2004

First Responders

(1) For months, state and local officials have been telling us that they need a reliable stream of funding from Washington in order to adequately plan and improve homeland security. Yet, the FY 05 budget represents a significant reduction from what Congress provided just last year - and even that amount is well below the needs that have been identified, especially by an independent task force sponsored by the Council on Foreign Relations. The task force found that current funding levels would leave us $98 billion short of what is needed to adequately prepare over the next five years. The President's budget also continues the trend of making deep cuts in the COPs program, in Local Law Enforcement Block Grants, and in Byrne grants, programs that local law enforcement especially rely on. How can state and local officials plan with any certainty, how can they know what to expect and adequately prepare with these large cuts being proposed in programs they rely on?

Answer: The Department of Homeland Security can not speak to Fiscal Year (FY) 2005 budget for the Department of Justice. It should be noted, though, that the President's budget request and the signed FY 2005 DHS Appropriations Bill include strong support for our Nation's emergency prevention and response community, which includes the country's more than 18,000 law enforcement agencies. Through the Department of Homeland Security's Office of State and Local Government Coordination and Preparedness, law enforcement agencies will receive substantial support from the $1.66 billion for the state formula grants program and the $885 million for the grants under the Urban Areas Security Initiative. As part of the state formula grants program, $400 million is for the Law Enforcement Terrorism Prevention Program (LETPP), which provides law enforcement communities with enhanced capabilities for detecting, deterring, disrupting, and preventing acts of terrorism. LETPP provides law enforcement communities with funds for a wide-array of activities, including information sharing to preempt terrorist attacks, target hardening to reduce vulnerability of selected high-value targets, threat recognition to recognize the potential or development of a threat, intervention activities to interdict terrorists before they can execute a threat, interoperable communities, and management and administration costs.

2. One of the most critical needs at the local level is for personnel. Fiscal crises have actually forced many localities to reduce the number of police and fire fighters – at a time when the threat from terrorism – as well as traditional crime – has increased. Yet, the Administration has proposed to virtually eliminate the COPs program, which has been used to hire 100,000 police officers and promote community policing. And the Administration has not provided funding in its budget for the SAFER Act, which Congress passed last year to provide funding for more fire fighters. Since police and fire fighters are often the first responders on the scene after a possible terrorist attack, their presence is essential to homeland security as well as to public safety. What is the Administration's rationale for cutting funding for these programs at a time when the need for police and fire fighters is so great?

Answer: As you know, with the support of the House and Senate Appropriations Committees, the Department of Homeland Security has administered dual funding programs – a formula-based state minimum program and a high-threat, high-density program – since Fiscal Year 2003. The Department and Administration firmly support this dual approach because it allows for baseline preparedness levels while targeting funds to high-threat, high-density urban areas across the country.

The Department and the Administration have also consistently supported an increase in funds for the high-threat, high-density urban areas program to meet the unique needs and challenges of the nation's urban areas. With the funds provided to the Urban Areas Security Initiative and the state formula grant program, the Administration's FY 2005 budget request supports both minimum levels of funding for states to continue their efforts to enhance security and targeted funds for the nation's urban areas.

The continuation of these efforts, and the $420 million increase in ODP's enacted level, coupled with the President's request for a 10 percent increase in funding for DHS as a whole, provides ODP, and the entire Department, with the resources we require to help secure the nation from acts of terrorism. The Administration and Department remain committed to providing our Nation's emergency prevention and response community the resources they need to continue to secure our Nation from future acts of terrorism.

In addition, the Administration and the Department recognize the importance of the support provided through the Assistance to Firefighters Grant Program, particularly with respect to rural.

3. The Public Safety Wireless Network has estimated that solving the problem of interoperability across the country could cost at least $18 billion. That amount clearly dwarfs the ability of state and local governments to deal with, especially given the fiscal crises they face. However, the budget actually eliminates the minimal funding that was targeted to interoperability in past budgets through FEMA and DOJ. I understand that other funding within ODP can be utilized for interoperability, however, that would mean a reduction in funds for protective gear, training, and other necessities. At the current pace, how long will it be before we achieve ubiquitous interoperability in our country?

Answer: The SAFECOM (Wireless Public Safety Interoperability Communications) program is currently working to develop a methodology to define and
measure progress on interoperability which will be used to establish a baseline of interoperability across the nation from which future progress may be measured. Interoperability is not a one-time goal but an iterative process that involves more than equipment procurement. Therefore, included is this methodology will be consideration of issues such as planning, maintenance, administration, training, and technology. As new technologies develop, they will need to link back to existing systems. As new challenges arise, they will need to work seamlessly with the current protocols and procedures in place. As a result, interoperability among emergency responders will be a continuing process that involves incorporating both technological and human factors.

The baseline will provide the government with the capability to assess the current level of interoperability as well as its incremental progress towards a minimum level of interoperability. This will allow for future estimates of nation-wide interoperability.

4. There is no doubt that funding for first responders has increased significantly since September 11. But that alone does not mean that we are now providing sufficient funds. An independent task force sponsored by the Council on Foreign Relations reported that the U.S. is on track to fall nearly $100 billion short of meeting critical emergency responder needs over the next five years. This estimate does not even include all police needs, because the Task Force could not obtain reliable estimates from police organizations. But it did identify a number of key needs. For example, the report noted that: "On average, fire departments across the country have only enough radios to equip half the firefighters on a shift, and breathing apparatus for only one third. Only 10 percent of fire departments in the United States have the personnel and equipment to respond to a building collapse." The report found cities without the means to determine whether terrorists had struck with dangerous chemicals or pathogens, and public health labs incapable of responding to a chemical or biological attack.

a) In putting together the Department's budget for first responders, did you meet with the authors of this report to try and understand why they have found such a huge gap between the resources in the budget and the needs on the ground?

b) If not, did you conduct your own needs assessment? What did that assessment conclude? Please provide copies of any needs assessments conducted by the Department. If no such assessment was done, what was the basis for the Department's budget for first responders?

Answer (Q01064 & Q01065): The Fiscal Year (FY) 2005 enacted level provides $33 billion for the Department of Homeland Security, building upon the significant investments to date that improve our safeguards against terrorism. Included in the FY 05 budget for DHS is $3.984 billion for the Office for Domestic Preparedness (ODP), which is the Federal government's lead agency responsible for preparing the Nation against terrorism by assisting States and localities reduce vulnerabilities against, prevent and respond to terrorist acts.

The FY 2005 enacted level is a significant commitment to providing funds to our nation's emergency prevention and response community, and continues the Administration's effort to secure the nation from acts of terrorism. The budget nearly doubles funds for the Urban Areas Security Initiative (UASI) effectively shifts funds away from arbitrary formulas to allocations based more on threat assessments. This will allow the Department to reinvigorate its commitment to providing homeland security funds based on terrorism risks, threats, and vulnerabilities. Included in the budget is $400 million for the continuation of the law enforcement terrorism prevention grant program, which focuses more funds on prevention and deterrence activities. Finally, the budget includes $715 million for continuation of the Assistance to Firefighters Grant Program. This is consistent with the Administration's FY 2004 request and provides significant funds for the continuation of this highly successfully and critically important program. The budget for ODP is at FY 2004 enacted levels providing significant funding for our Nation's emergency prevention and response community.

ODP has received homeland security strategies from all 50 states, the District of Columbia These strategies were due on January 31, 2004, as a requirement for the States and territories to receive and distribute FY 2004 ODP funds. These strategies lay a strategic vision for homeland security within each State, territory, and urban areas, supported by measurable goals and objectives. Collectively, they represent an overall road-map for improving preparedness nationally, and provided an extensive set of data regarding State and local vulnerability, risk, and capabilities. The strategies are also an invaluable resource to assist ODP and its partners in better allocating federal resources for homeland security. The information included in these strategies will provide the Department additional information to determine national threats, vulnerabilities, and needs.

5. At the hearing on February 9, you testified that there is $8 to $9 billion in funds for first responders "still to be distributed." You stated that some of the funds from FY 02 have not been distributed, along with almost half of the funds from FY 03 and additional funding from FY 04. As you know, the time it takes for these funds to reach the front lines has been and continues to be a source of frustration for mayors and first responders and is a key reason why many support providing funds directly to those on the front lines, rather than through the states.

a) Your statement tends to confirm the mayors' contention that the current process for distributing these funds is simply not working. Given that, why does the Department continue to oppose efforts to provide more funding directly to local governments, especially those in large metropolitan areas who clearly have the capacity to manage funds as effectively as states?

Answer: The Administration and the Department of Homeland Security are opposed to providing funds directly to regions and localities. By providing funds directly to the States, as is current practice, the Department can monitor how federal funds are being spent and ensure that spending follows federal regulations and guidelines.

Additionally, providing funds directly to the States allows each State to distribute funds and assistance in a planned and coordinated manner to not only meet the national

homeland security needs but also to coordinate and facilitate funding to meet state and local need.

Congress already has shown its support for this approach by requiring States to complete comprehensive needs and vulnerabilities assessments and statewide domestic preparedness strategies. Through the assessment and strategy development process, States can readily plan for current and future equipment purchases. This benefit would be lost if funds were provided directly to regions or localities.

b) What is DHS doing to track and monitor the distribution of homeland security funding so that we know with some certainty how much has been distributed to states, how much has been passed-through to the local level, and how much remains in the pipeline?

Answer: For the FY 2003 State Homeland Security Grant Program (SHSGP), Part I and II and Urban Areas Security Initiative (UASI) Part I and II grants, ODP's grant guidance notes that states were expected to obligate 80% of equipment funding for SHSGP I, 80% of first responder preparedness funding in SHSGP II, 50% of CIP funding in SHSGP II, and 80% of all funding for the UASI II program to units of local government within 45 days. To that end, ODP set up a follow-up system whereby ODP would notify the state 10 days out from the 45th day (via a letter) that ODP expects states to certify that they had obligated these funds. The certification was done via a "fax back" form to their ODP preparedness officer. On the 46th day after the grant award, we sent out a letter reminding them of the obligation requirement, with an accompanying fax back form that required them to certify that they had met this obligation requirement, and to further explain (through a narrative) how the funds were being used.

We received a majority of the fax backs within the allotted time, and ODP is relying on the certification of those states that they have met the statutory requirement. For states that did not provide the information, or noted that they did not comply, we provided a number of options. ODP offered technical assistance to help them comply with certification. In other cases, states notified us of a date they would be in compliance (in some states, legislatures and other elected bodies need to meet so that can hold up federal funding obligation). The last resort for states who did not comply was the notification that ODP intended to put a hold on the state portion of their funding until they came into compliance.

In Fiscal Year 2004, the Homeland Security Grant Program and the Urban Area Security Initiative grantees will certify their obligations through the Initial Strategy Implementation Plan (ISIP), which is due 60 days after grant award. The grantees will submit this form to ODP, and failure to submit the form will cause funding to be administratively held, as noted in the special condition in the grant.

c) Beyond consolidating key funding programs within the Office of Domestic Preparedness, what else is the Department doing to cut through red tape and get funding to the local level as quickly as possible?

Answer: The expeditious award and obligation of homeland security funds is an overarching goal of the Department of Homeland Security. Nevertheless, there are a number of factors that may be causing delays in award and draw-down of funds, which can vary across states and jurisdictions. For instance, a number of states require there state legislature to include the federal grant in their state budget in order to accept and receive the award. Further, many states have biennial budgets, which could further complicate the receipt and award of federal funds. Another potential chokepoint is the limited number of pieces of specialized equipment. The increased demand for products creates manufacturer backlogs and subsequent delays in delivery and receipt of equipment.

The Department has taken immediate steps to expedite and facilitate the award and draw-down of homeland security funds. For instance, DHS, through the Office for Domestic Preparedness (ODP), streamlined the grant application process by eliminating the preliminary review of budget information and implementing new reporting and monitoring mechanisms to make funding available immediately upon grant award. Previously, local jurisdictions faced two layers – state and federal – of budget worksheets before they could access funds.

The Department is working to get a better idea of the reasons for delays in obligating and spending homeland security funds. As such, the Secretary formed the Homeland Security Funding Task Force to examine this issue and offer recommendations on how to address the problems with delays. The Task Force submitted their report, "A Report from the Task Force on State and Local Homeland Security Funding," which contained a number of recommendations to expedite the money distribution process. The Department is currently reviewing the report, but will continue to work to ensure that homeland security funds are distributed efficiently and effectively.

Operation Safe Commerce

6. Operation Safe Commerce (OSC) was initiated to fund pilot programs to see how effectively and efficiently we could track containers. We learned a lot in the first few phases. Some of the vulnerabilities we observed in the supply chain by tracking containers we expected and confirmed; others were new to us. Yet the FY05 budget request includes absolutely no money for OSC. So not only can we not expect the program to look forward, it can't even continue its current mission. Why did one of the Department's most innovative port/container security programs receive no money in the President's FY05 budget request?

Answer: As you know, Operation Safe Commerce (OSC) is a collaborative effort between the federal government, the three largest U.S. container load centers (Los Angeles/Long Beach, Seattle/Tacoma, and New York/New Jersey), private industry, and the maritime community to develop and share best practices for the secure and expeditious movement of containerized

cargo. OSC's goal is to serve as a test bed to examine methods to increase supply chain security, protect the global supply chain, and facilitate the flow of commerce. The Administration continues to administer OSC in FY05 as a multi-agency program with participants from the Departments of Homeland Security, Transportation, State, Commerce, and Justice. An Executive Steering Committee (ESC) was formed to provide guidance for OSC. The ESC is co-chaired by the Transportation Security Administration, Bureau of Customs and Border Protection, and the Department of Transportation.

Congress has provided $75 million for this program over a three-year period to conduct very robust and comprehensive pilots through the selected locations. Over a one year period, integrated teams assessed supply chain security and implemented solution sets in the real world environment. These solution sets included technology (such as e-seals, tamper evident tape, radiation detectors, sensors, biometric credentialing, tracking devices, and through the wall radar) as well as, business practices (such as third party inspections and document authentication) addressing security requirements. To date, more than 800 containers have been tested in the pilot projects through the 3 container load centers. Two of the load centers (New York/New Jersey and Seattle/Tacoma) have completed all of their pilot projects, while the third (Los Angeles/Long Beach) is scheduled to complete all testing by December 31. OSC is now entering into it's third phase. This phase focuses on enhancing and extending the accomplishments of the earlier phases. For this phase, the Office for Domestic Preparedness (ODP) is seeking proposals that address (examines and test potential solutions) security throughout the entire global supply chain from point of origin to point of destination.

On May 16, 2004 the Operation Safe Commerce program was transferred to the Office for Domestic Preparedness from the Transportation Security Administration. ODP plans to manage OSC as a federally funded, innovative public/private partnership dedicated to enhancing security throughout international and domestic supply chains while facilitating the efficient cross-border movement of legitimate commerce.

Border Personnel, Visas, U.S. Visit

Border Personnel

7. In the Patriot Act and subsequently in the Border Security Act, Congress authorized the hiring of additional inspectors and investigators at Customs and INS. Almost none of these goals have been met. Furthermore, a Congressionally chartered task force examining border issues [the Data Management Improvement Act Task Force], made up largely of DHS and other agency officials, stated this December that "insufficient staffing is universally recognized as one of the most critical issues that needs to be addressed." In December 2003, the Department announced that it had achieved one of the Congressional directives by deploying 1,000 Border Patrol agents on the Northern border. This goal was reached, however, by reassigning many agents from the Southern border. Are we merely robbing Peter to pay Paul?

Answer: The number of agents on the northern border had been increased to 1,006 as of the end of December 2003. This is triple the number of agents that were assigned along the northern

border prior to 9/11 and meets the Patriot Act's requirement for staffing on the Northern border. The number of agents currently assigned to the northern border remains at 1,006.

The agent increase was accomplished through the permanent relocation of experienced agents from across the nine southern border sector areas. The CBP budget has sufficient funds to backfill the agent vacancies through a combination of new agent trainee hires and the relocation of experienced agents among the southern border areas. The relocation of agents from the southern border to the northern border was initiated in order to increase the agent staffing on the northern border in the most expeditious means possible and to provide the northern border sectors with experienced and tenured agents. The southern border sectors have the training infrastructure already in place to absorb large increases in agent trainees without compromising the integrity and strength of their agent force during the assimilation of the new agents. The northern border sectors lacked the capacity to bring large numbers of trainees up to an acceptable experienced level without adversely affecting their current operational abilities. Thus, Peter shared his vast wealth of experienced agents with Paul in order that border control was enhanced on the northern border while maintaining the higher level of border control along the southern border.

8. Why does the FY05 budget call for a decrease of $18 million in funding for border security and control personnel between ports of entry?

Answer: The change in funding from FY 2004 to FY 2005 does not represent a decrease in the level of effort for Border Patrol. Included in this change are adjustments to maintain current levels, program increases in FY 2005, the annualization of Congressional Action, deduction of one-time costs from FY 2004, deduction for the FY 2005 Cost Savings Initiative, and a deduction for Enhancements not received in the FY 2003 Appropriation.

Visas

9. The September 11th Commission recently reported that before the 9/11 attacks, screening procedures at our consulates were not designed to look for potential terrorists. They checked names of applicants against a watch list of terrorists, but they did not receive any training whatsoever in looking for suspicious signs during interviews, nor did they receive any available information about looking for suspicious travel documents. The screening process was geared primarily towards detecting people who may be planning to immigrate unlawfully to the U.S.

a) What are you doing to enhance the ability of consular officials to screen for potential terrorists?

Answer: Section 428 of the Homeland Security Act directs DHS to conduct visa security operations at visa-issuing posts worldwide. This includes deploying officers overseas to review visa applications (including 100% of visa applications submitted in Saudi Arabia), providing advice and training to consular officers, and initiating investigations pertaining to Section 428 responsibilities. DHS has established a Visa Security Unit (VSU), within the Bureau of Immigration and Customs Enforcement (ICE) Office of International Affairs, to conduct these

visa security operations. DHS initiated visa security operations at two posts in Saudi Arabia in October 2003. At those posts, DHS officers have been reviewing all visa applications; providing guidance and ad hoc training to consular officers on document review methods, imposter detection, and interview techniques; and providing assistance to other law enforcement agencies at post.

VSU recognizes the importance of enhancing consular officers' ability to screen for potential terrorists. In addition to the ad hoc training and advice that visa security officers provide consular officers at post, VSU plans to develop formal training for delivery both at post and centrally at the National Foreign Affairs Training Center. In doing so, VSU plans to draw extensively from the experience of ICE visa security officers deployed to visa-issuing posts. Those officers will observe consular operations, assess consular officers' training and skill sets, and provide input and guidance on training development based on the needs they have identified in the field.

b) Are there specific programs in your budget to address this?

Answer: The FY2005 budget includes $10 million in the Immigration and Customs Enforcement request. This amount would fund the training programs and visa security initiatives in Saudi Arabia and other over seas locations. In FY 2004, the VSU will maintain the existing Saudi operations and will continue to rely on temporary detailed personnel to fill all staff roles. The absence of FY 2005 funding will prevent DHS from expanding operations to additional posts, which will impair its ability to develop comprehensive, appropriate, and relevant training for consular officers.

10. There is a concern that the Department's plans for tracking departures under the US-VISIT program may well be ineffective. For example, foreign visitors will be expected to remember to check themselves out at unmanned automated kiosks inside airports. Once they have done so, there is no guarantee they will not leave the airports and stay in the US, as international departure lounges are not separate in American airports. Can we expect all foreign visitors to use the automated kiosks when they leave? How will the Department ensure that foreign visitors actually leave the country?

Answer: US-VISIT is piloting several possible exit solutions. Currently, all foreign visitors who are required to complete the US-VISIT process upon departure provide their biometric and biographic information at a kiosk that has oversight by a US-VISIT contracted Work Station Attendant (WSA). The verification of departure is completed when the traveler boards the vessel and the manifest is submitted and matched against the US-VISIT information from the kiosk. The US-VISIT program, as required by the 5 January 2004 US-VISIT regulation, will pilot and evaluate other technical solutions that will be able to biometrically verify the traveler's departure at the gate area prior to boarding. This will assist in addressing the concerns that the visitor may chose not to use the exit kiosk.

The other solutions being piloted require foreign visitors to check out with a US-VISIT WSA at the port departure gate. Foreign visitors will go though one of the following processes, depending on location.

- Under one alternative, visitors departing the United States will check out of the country at the exit kiosk located within the airport or seaport terminal. As with the process the visitors encounter upon entry at airports or seaports, their travel documents are read, their two index fingers will be scanned at the exit kiosk, their digital picture will be taken, and they will receive a printed receipt that verifies that they have checked out. A WSA will be available to assist with visitors' check-out.

- The second alternative requires the visitor to check out at an exit kiosk, but will require the visitor to present the receipt to the WSA at their departure gate to validate that she/he checked out at the exit kiosk. The WSA will use a hand-held device that will scan the machine-readable zone on the receipt for the biographic information and photo of the traveler, then require the visitor to place one finger on a finger scan (attached to the device). The device will verify if the finger scan is the same as that of the finger scan on the receipt. The visitor is allowed to board the vessel after completion.

- Another alternative under the pilot program is a biometric check-out process with a US-VISIT exit attendant at visitors' departure gates. The visitor is not processed at the exit kiosk, but at the departure gate by a WSA during the boarding process. The WSA will use a hand-held mobile device that is able to scan the passport, take two finger scans and a photo, and print a receipt for the visitor. The mobile device sends the information immediately to the DHS network to check against the biometric watchlist for matches.

Information is being provided to visitors to make them aware of the requirement to record their departure, where there is exit capability. To help the process run smoothly, foreign visitors will receive a printed card explaining the exit process from Customs and Border Protection when they arrive in the United States. Many transportation companies have been informing travelers of the requirement upon check-in. Also, directional signs are strategically located throughout the airports and seaports.

The exit pilot during the next few months will evaluate a variety of areas such as the visitors' compliance rate and the different mechanisms conduciveness to travel, such as ease of use, location, time to process, and cost.

11. How do you respond to concerns that the Department is proceeding with US VISIT without yet having an adequate plan for how the technology will work?

Answer: The technology solutions being implemented by US-VISIT to support the 2003 and 2004 mandates are primarily integration initiatives to make interoperable a number of legacy systems and the associated data. The program office thoroughly understands the technology investments required and the capabilities of the integrated solutions. As US-VISIT moves forward, future technology development will follow formal system development life-cycle requirements, and will be aligned with Departmental solutions and standards.

Transportation Security Administration

12. The President's budget highlights the request for $900 million in additional funding for TSA in FY05. However, these new funds will be used to pay for costs for existing programs, not to undertake new transportation security initiatives. Although TSA has made important strides in improving aviation passenger and baggage screening, more must be done to close other serious gaps in aviation security. What new aviation security programs or countermeasures will TSA be able to implement in FY05, if any, under the proposed funding levels?

Answer: As you acknowledged, the TSA has made important strides in improving aviation passenger and baggage screening since its inception and TSA's top priority remains transportation security. Consequently, DHS and TSA must continue to balance many competing priorities and the optimal use of available funding to ensure stability and consistency in all programs, particularly aviation security. The roughly $900 million increase for the TSA represents a 20 percent increase over FY 2004 funding. For FY 2005, we are expecting to strengthen the existing interwoven, concentric layers of security established in previous years. The majority of the requested increase includes funding to support ongoing research and development in air cargo security and next generation electronic screening technologies and funding to operate and maintain our significant investment in screening technology at the nation's airports.

TSA continues to develop new layers of aviation security measures. In FY 2005, we are planning to implement decisions regarding the Transportation Worker Identification Credential (TWIC) prototype, the expansion of the Federal Flight Deck Officer program to include cargo pilots, and the Secure Flight program. We will also continue the systematic deployment of information technology to the Nation's airports, which will enhance information flow to and from airports and our aviation security workforce

13. At the February 9 hearing, I asked you how TSA's $24 million budget request to maintain the level of personnel assigned to address security in non-aviation transportation modes would allow TSA to expand its efforts to improve security beyond passenger aviation. You stated that Congress had provided the bulk of TSA's appropriation for aviation and that funding available through the Coast Guard and the Information Analysis and Infrastructure Protection Directorate, among others, would address these other modes. You also indicated that other Departments should work to secure certain modes of transportation.

a) As you know, TSA is responsible by law for security in all modes of transportation, not just aviation. Why hasn't the Administration requested funding to allow TSA to fulfill this important aspect of its mission?

Answer: Ensuring that our nation's transportation systems are secure must be accomplished through effective partnering between appropriate federal, state, local and private industry entities. Although TSA was created in the wake of the September 11 attacks and charged with responsibility for ensuring that all modes of transportation are secured, the Administration has consistently held that that this

responsibility must involve the coordination of appropriate federal, state, local and private industry partners, many of whom were already in the business of providing security for their particular piece of the transportation puzzle. TSA's main charge, both under ATSA and now as part of the DHS family, is to coordinate these efforts under the guidance of the Secretary and the Under Secretary for Border and Transportation Security, identifying gaps and working with appropriate partners to ensure that existing security gaps are filled.

Recognizing this, the Department of Homeland Security (DHS) has requested substantial resources in FY 2005 across the agencies within the Department involved with securing transportation modes other than aviation, including resources in the Coast Guard and CBP for ports and maritime security; in Customs and Border Protection (CBP) for cargo security; in Information Analysis and Infrastructure Protection (IAIP) for vulnerability assessments, intelligence, and infrastructure protection for all sectors including transportation; and in Emergency Preparedness & Response (EP&R) for emergency response to only name a few. In addition to working with other DHS components, TSA works closely with our sister Federal agencies outside of DHS to ensure that government resources are maximized. For example, under the leadership of BTS and DHS, TSA is coordinating key standards-setting efforts in areas such as transit and rail security, and is working closely with modal administrations of the Department of Transportation to help leverage their existing resources and security efforts to accomplish security goals.

b) What specific initiatives will TSA pursue in FY05, if any, to improve non-aviation transportation security?

Answer: In partnership with other DHS component agencies and the Department of Transportation (DOT) modal administrations, TSA is identifying security vulnerabilities in the non-aviation modes of transportation for use in developing and implementing, as appropriate, national performance-based security standards to improve the security of passengers, cargo, conveyances, transportation facilities and infrastructure. TSA is also working closely with those partners to ensure compliance with established regulations and policies.

Specific projects TSA is undertaking or that are under discussion include:

- Partnering with IAIP and industry stakeholders to leverage Information Sharing Analysis Centers effectively;
- Assessing hazardous materials (HAZMAT) transport security threats and identifying best practices and mitigation strategies to secure HAZMAT transport through High Threat Urban Areas (HTUAs);
- Working with the Science and Technology directorate to develop chemical, biological, and radiological countermeasures for engaging and defeating attacks in mass transit settings;
- Assessing the operational feasibility and appropriateness of applying tailored screening standards to passengers in non-aviation environments;

- Working under the guidance of the Border and Transportation Security Directorate, and with U.S. Customs and Border Protection (CBP) and the USCG to develop the appropriate framework for securing the intermodal transport of containerized cargo in the domestic United States.
- Working with DOT, USCG, and public/private transportation operators to ensure that transportation security planning efforts are aligned with IAIP's Critical Infrastructure Protection Plan.

On March 22, DHS announced the following initiatives for rail and mass transit.

- Continued engagement with industry and State and local authorities to establish base-line security measures based on current industry best practices;
- Transit and Rail Inspection Pilot (TRIP) to test the feasibility of screening luggage and carry-on bags for explosives at rail stations and aboard trains;
- The integration of existing public and employee awareness programs and the creation of new programs where necessary; and
- Investment in the research and development of technological innovations for biological, chemical, and high explosives countermeasures.

14. The Administration has announced plans to transfer grant programs for Operation Safe Commerce, intercity bus security and trucking security from TSA to the Office of Domestic Preparedness, but is not requesting any money for these programs.

a) What, then, exactly, is being transferred?

Answer: TSA and the Office of Domestic Preparedness (ODP) have met several times to discuss the potential transfer of transportation security grant programs to ensure a seamless process for grant applicants. ODP is moving towards becoming the "one-stop shop" for Federal support of homeland security initiatives that state and local governments so desire. The intent behind the proposed transfer of security programs is to simplify the administration of the grants and thereby strengthen communication with and support for state and local governments. TSA will assist in providing both technical expertise and process facilitation for transportation security grant programs. The proposed transfer would be effective for FY2005 and beyond.

b) What is the Administration's view of the federal role to help secure intercity buses, trucking, rail and other modes of transportation?

Answer:

The Department views transportation as a shared public-private responsibility and will continue to work with industry stakeholders and the Department of Transportation (DOT) modal administrations to ensure that Federal security grants facilitate the seamless integration of industry and regional, as well as state and local, security planning.

TSA and the Office of Domestic Preparedness have previously provided significant resources to the public and private sectors through both competitive grant programs, and the Urban Area Security Grant program, for security enhancements to the transportation system. For example:

- Privately owned facilities were the recipients of just over 50% of the project funds in ***port security enhancement grants*** – reflective of the fact that the majority of regulated maritime facilities are privately owned.
- ***Bus security grant*** funding provided by Congress in the FY02, FY03 and FY04 appropriations was specifically targeted for privately owned over-the-road buses.
- ***Highway Watch Grant*** funding in FY03 and FY04 is targeted for the industry led truck security program.
- ***Operation Safe Commerce*** funding for study of cargo supply chain security was targeted for the three major load centers, which are a combination of state, regional and bi-state management.
- ***Urban Area Security Grants*** awarded in FY 03 and FY 04 provide $115 million to state, local, and regional transit operators for security improvements.

Watch lists and guns

15. DHS is responsible for generating and overseeing a number of terrorist watch lists. For example TSA maintains the so-called "no fly" watch list, and if someone appears on that watch list, they are prohibited from getting on an airplane in the United States. Presence on any of those watch lists, however, doe s not currently have any impact on someone's ability to buy a gun in the United States. In other words, individuals who DHS thinks are such dangerous terrorists that it won't allow them to get onto a plane, among other things, can still go into a gun store and buy a gun, unless they fit into one of the other categories of people who aren't permitted to buy guns.

a) Do you believe that all terrorist watch lists should be among the indices checked when someone is seeking to buy a gun?
b) Do you believe that presence on any or all of the terrorist watch lists should disqualify someone from purchasing a gun?
c) Even if you believe that presence on any or all of the watch lists should not automatically disqualify someone from purchasing a gun, should it lead to some lesser consequence, such as a waiting period?
d) Even if you believe presence on any or all of the watch lists should not impact on one's ability to purchase a gun, do you think the agency that put the individual on a watch list should be notified if someone on a watch list seeks to buy a gun and that the agency should be informed of where the individual is?

Answer (a-d): Recommend you refer these questions to TSC.

Information Sharing

16. The discovery of ricin in the Majority Leader's office last week was followed by revelations that the Secret Service actually withheld information from the FBI and other agencies about the discovery of a ricin-contaminated letter addressed to the White House in November. It seems incomprehensible that after all of the focus on the need to share information about terrorist threats, that the Secret Service had information about a potential terrorist attack on the White House, yet chose not to share it for almost a week with the FBI and with others who clearly have a need to know – including the Postal Service which has a responsibility to protect employees. I understand that new procedures have been put in place to avoid a similar delay in the future – but the fact that this continues to occur is disturbing.

(a) As the lead Administration official on homeland security and as the cabinet secretary responsible for the Secret Service, when did you find out about the White House incident?

Answer:

DHS was notified of the letter on November 12, 2003. However, it is important to provide clarification of several inaccuracies included in the initial media reports detailing this matter.

On Thursday, November 6, 2003, a letter addressed to the White House arrived at an offsite mail handling facility after having already completed an irradiation process. Based on its appearance and contents, the letter was pulled aside. This is not an uncommon practice as this facility processes a high volume of suspicious letters and packages. An initial field test was performed on the letter with negative results. On November 7, a test of the sorting hoods detected positive traces of ricin, triggering a battery of additional and more sophisticated tests. All of these tests, performed over the next few days with mixed or inconclusive results, were conducted by leading chemical and biological experts from the Department of Defense. On November 12, several agencies were notified of this discovery, including DHS, the FBI, the U.S. Postal Inspection Service, and the Department of Transportation, which had been investigating a similar incident in South Carolina.

On November 13, the Homeland Security Council led a number of interagency discussions about this matter and a unanimous decision was made to transfer the letter and its contents to the FBI for transport to the Centers for Disease Control and Prevention (CDC) for additional testing. These tests revealed traces of ricin, but levels that were determined by the CDC to pose no risk to public health. The letter has since been the subject of investigation by the FBI.

It should be noted that the Secret Service receives threats against the White House in a variety of forms every day. In every instance, a judgment must be made about the validity of these threats and the appropriate response, including the possible involvement of other law enforcement entities and the public health community. The Secret Service is continually evaluating the changing threat environment, modifying its preventive

measures and threat management procedures, and adapting as necessary. Immediately following this incident in November, the Secret Service reviewed existing notification procedures and determined that improvements could be made. The applicable protocols have subsequently been adjusted, and there is a strong commitment to ensuring that earlier notifications are provided should a similar incident involving a biological/chemical agent occur in the future. However, due to the complexity of the testing procedures, such earlier notification will have no impact on the length of time required for a determination to be made of the unknown substance.

b) Did you take any preventive, pre-cautionary, or warning measures when you became aware of it?

Answer:

The Department took immediate steps to ensure that all appropriate law enforcement and public health agencies were notified of the discovery. The contents of the letter were subsequently deemed no risk to public health by the CDC, and the FBI has continued its investigation.

c) Have you learned exactly why the Secret Service chose to delay notifying the FBI and others?

Answer:

As stated earlier, the detection of unusual letters and substances addressed to the White House is not uncommon. As with all potential threats made against the White House and Secret Service protectees, the Secret Service must exercise its judgment in determining the validity of a threat and the appropriateness of notifying other agencies. In the case of the offsite mail processing facility, the Secret Service collaborates with leading chemical and biological experts from the Department of Defense to determine the nature of an unknown substance. With this incident, a series of tests were performed to determine the nature of the substance, and, once those tests were completed, all appropriate law enforcement and public health agencies were notified. Regardless, the Secret Service has modified the applicable protocols to ensure earlier notification after such a substance has been detected.

17. What have you done to re-enforce the criticalness of sharing information within DHS and between DHS and other agencies? Have any directives been issued to this effect?

Answer: Within weeks of the creation of the Department, I and the heads of the main Federal home-land security agencies signed a memorandum of understanding that clearly established a new policy that favors sharing of terrorist information. Again last September, we established cooperative procedures to set up the Terrorist Screening Center, pooling human resources and mandating sharing of consolidated terrorist watch-list information with the various screening and law-enforcement systems in DHS, Justice and State, and used by both Federal and local officials. The TSC has already shown tangible results from this joint approach. I have directed the IAIP Undersecretary to establish a Departmental Information

Sharing program, and directed the DHS CIO to support that initiative. On the One-Year anniversary of the Department, we announced a number of information-sharing initiatives, including initial deployment of the first component of the Homeland Security Information Network, with more to follow this year. Our new Strategic Plan also identifies information sharing as a DHS priority.

18. The Markle Foundation issued a report a few weeks ago which took a broad look at information-sharing and concluded that the information-sharing regime which served us during the Cold War, when the premium was on securing information, is no longer adequate now when we need to share information in order to keep Americans safe. One of its recommendations is to measure agencies performance and judge them on how well they share information.

a) Do you agree with this recommendation?

Answer: The second report of the Markle Foundation's Task Force on National Security in the Information Age ("Creating a Trusted Network for Homeland Security", December, 2003) offers many good recommendations, including the idea of measuring progress in information sharing. We agree that measuring performance is essential, and we are establishing performance metrics for all our strategic goals.

b) Do you have any plans to implement it, or other recommendations from the Markle Task Force, within DHS?

Answer: Many of the Task Force recommendations are consistent with our plans and initiatives. For example, in the technology area, we are establishing a program to standardize data formats and definitions so that we can more effectively share it within DHs and with external partners (see Report, p.14). We also agree that DHS should take the lead in collaboratively designing a decentralized network with strong and flexible authentication and permissions management facilities. (Report, p. 21/21.)

19. From discussions with officials at TTIC and DHS, it is not at all clear how many briefs the President receives each day on terrorist threats and homeland security, or who briefs him. I would appreciate any general information you can provide to clarify this issue, as well as your response to the following questions.

a) In the FY05 Congressional Budget Justification, the Homeland Security Operations Center at DHS is described as providing a daily "Situation Brief for the President" because the Center is meant to be the single point of integration for homeland security information from federal, state, local and private sources. Is the "Situation Brief" produced every day by the Homeland Security Operations Center at DHS?
b) Is the "Situation Brief" provided to the President daily?
c) Who provides this briefing?
d) What other briefs on homeland security and the terrorist threat are done for the President either on a daily basis or periodically?

Answer:

The HSOC provides a briefing team and an integrated Intel (from IA) and OPs (HSOC) briefing product to the Secretary each morning prior to his meeting with the President. It normally goes at the WH about 0730 prior to the Secretary's 0800 with the President. In addition, six days per week, the President receives and is briefed on the President's Terrorist Threat Report; a joint product produced by TTIC with input from DHS and other members of the Intelligence Community.

DHS also participates in secure video teleconferences twice per day with the White House and other Intelligence Community officials and participates in meetings of the Counterterrorism Support Group twice per week. When requested, DHS also provides briefings on current threats and protective measures to White House officials.

Bioterrorism Budget

20. The Secretary's February 9th testimony on the FY'05 budget states that funding for the purchase of bioterrorism countermeasures (vaccines, medicines, etc.) under Bioshield Program is increasing by 186% (from $890 million in '04 to $2.5 billion in '05.) In fact, the $2.5 billion claimed by the Administration for '05 is part of $5.6 billion advance appropriation provided by Congress last year to cover the Bioshield Program needs through the year 2013. In particular, the $2.5 billion claimed by the Administration as a one-year increase for '05 was actually appropriated by Congress to cover Bioshield funding needs for the next four years (2005 through 2008). DHS budget tables provided by OMB, in fact, show expected obligations for this program in FY'05 to be only $895 million or essentially the same as FY'04.

a) Does DHS agree with the OMB estimate of FY'05 obligations? If not, what level of obligations does DHS expect to achieve in FY'05?

   Answer: Yes, DHS does agree with the OMB estimate. Plague, Ebola and other hemorrhagic fever products will not be available until FY05 – FY07, and procurement decisions will require refinement of requirements and cost estimates over the next months. The nature of research and development is a significant factor in the ability to procure products. As a result, the exact timing cannot be determined. One major component of the BioShield program is its ten-year life cycle, in recognition of the fact that there is uncertainty of the time/progress factor in research and development. Additionally, the emergence or re-prioritization of threats may require funds to be redirected to either different or more urgent projects.

b) At this point in time, what level of obligations does DHS actually expect to achieve in FY'04?

   Answer: For FY 2004, DHS obligated $884,749,000.

21. ***Bio-Surveillance Enhancements*** -- On January 29, DHS Secretary Tom Ridge and HHS Secretary Tommy Thompson held a joint press conference (prior to the public release of the budget) touting a new $274 million program to improve the Nation's bioterrorism surveillance capabilities." According to the press release accompanying this announcement, DHS "will use $129 million to undertake two significant enhancements to its current bio-surveillance efforts." (emphasis added) The release, in turn, identifies only two enhancements – $11 million to the Department's Information Analysis and Infrastructure Protection division (IAIP) to develop a real-time system for harvesting data" and $65 million to the Department's Science and Technology division (S&T) "to enhance current environmental monitoring activities." The Secretary's February 9 testimony similarly discusses only the $11 million for IAIP and the $65 million for S&T. These account for only $76 million rather than $129 million.

a) Please identify the Department's allocation of the remaining $53 million in "enhancements to its current bio-surveillance efforts."

Answer: The President's FY 2005 Budget Request for the BioSurveillance Initiative is both for continuation of on-going bio-surveillance activities and for their enhancements. The $53 million mentioned is in fact the cost for running the current baseline BioWatch Program in more than 30 cities across the Nation. The proposed enhancements would then build upon this baseline system.

22. ***Bio-Watch Program*** -- The Secretary's February 9 testimony states that one key component of the expanded bio-surveillance program is the "expansion and deployment of the next generation of technologies related to the Bio-Watch Program, a biosurveillance warning system."

a) Please identify how much of the $129 million in total funding is being applied to each of these two activities – (1) the expansion of the biosurveillance system, and (2) the development of new next-generation technologies.

Answer: The referenced FY 2005 budget request for $129 million contains two separate areas: in the S&T Directorate, funds for the continued operation/enhancement of the BioWatch System ($118 million); in the Information Analysis and Infrastructure Protection (IAIP) Directorate, funds for a National Biosurveillance Systems Integration System.

A detailed break down of the FY 2005 budget request is as follows:

BioWatch (S&T, $118 million)
1) BioWatch current baseline operations/sustainment (installed in major cities) - $53 million.
2) Expansion of the current BioWatch system - relates to the dramatic expansion of the number of sample collectors in the highest threat cities and at high value targets such as stadiums and transit systems - the request in this area is for $34 million.
3) Development of next generation technologies for BioWatch -this area includes advanced

detection systems and software tools for attack warning and characterization in BioWatch cities - $31 million
4) BioWatch funding recap - $53 million for operations, $34 million for expansion and $31 million for next generation – total of $118 million S&T request

National Biosurveillance Integration System (IAIP. $11 million)
In IAIP, $11 million is included to integrate, in real-time, bio-surveillance data collected from sensors throughout the country and with disease and contamination surveillance and health reporting information from human health, animal, water, wildlife and international monitoring system now in place and those in development. Our new National Bio-Surveillance Integration Center, to be deployed within IAIP, will fuse these various information streams to create a ground breaking, new national biological situational awareness capability. This capability will enable the Department of Homeland Security to provide a common operating picture, shared across the health, agriculture, water and food Sector Specific Agencies, which can also be analyzed within the context of terrorist-threat information from the law enforcement and intelligence communities. This capability will enhance the nation's ability to detect, characterize and attribute a biological attack, as well as guide the appropriate response in order to mitigate its consequences.

b) Within the physically deployed Bio-Watch system, as distinct from the technology development efforts, please describe which deployment and operating costs are currently paid for by DHS and which costs, if any, are paid for by state and local government agencies within whose jurisdiction the system is deployed.

Answer: Currently all deployment and operating costs for BioWatch are paid for by DHS.

c) Will there be any changes in the allocation of costs to state and local governments in the expanded Bio-Watch program proposed in the FY'05 budget?

Answer: No, there will be no changes in the allocation of costs to state and local governments in the expanded BioWatch program proposed in the FY 2005 budgets. All operating costs will continue to be paid by DHS.

d) What will be the total annual operating cost of the expanded Bio-Watch program and how much of that will be covered by the DHS?

Answer: The total annual operating cost for the expanded BioWatch system will be $87 million per year, with all of it covered by DHS.

e) How much of the total $129 million funding supports on-going Bio-Watch activities such as the first-generation system that has already been deployed?

Answer: As noted in Question Q01090 above - $118 million of the FY 2005 S&T budget request is related to BioWatch. Of the $118 million, $53 million is for the operation of the first

generation BioWatch system that has already been deployed. The $11 million for IAIP funds development and deployment of a capability providing real-time integration of multi-agency data streams with threat information. This will enhance the nation's biological situational awareness and improve our ability to detect, characterize and respond to possible attacks on our population, agriculture, food, and water supplies in a coordinated manner.

f) How much of the total $129 million funding supports state and local government planning and preparation to respond to both positive and false positive findings from the monitoring system?

Answer: The BioWatch request includes $2 million to support state and local governments in the area of consequence management.

Critical Infrastructure Protection

23. GAO and many others have noted that a comprehensive assessment of the threats and risks to our critical infrastructure are vital to target our prevention and protection efforts wisely, to make sure that we are addressing those areas first which – if attacked – pose the greatest risk to the health and safety of the public and to our economy. Yet, work on producing detailed risk and vulnerability assessments appears to be lagging. I have long been concerned about our planning to protect critical infrastructure and have written to you twice on this matter – on March 19, 2002 and again on March 20, 2003. In a September 4, 2003 response to the second letter, Under Secretary for Information Analysis and Infrastructure Protection Frank Libutti indicated that some initial assessments had been made, and others were "underway" or being planned. This vague response was not responsive to my request for a detailed update on the status of assessments and planning for various critical infrastructure sectors. In addition, in December the President issued Homeland Security Presidential Directive #7, which gives you another year to generate "a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources." This is the type of planning many of us believed had already taken place – or should have.

Please indicate, as specifically as possible, the status of threat and vulnerability assessments of critical infrastructure sectors and key assets. In particular, please describe:

a) The nature and extent of work done thus far on risk and vulnerability assessments.
b) The nature and extent of work planned under HSPD #7 and how this will differ from the work done to date. What is the deadline for this work? Do you anticipate it being completed before the one-year deadline provided by the Directive?
c) Any specific increases in the FY 05 budget that will help move this process forward more quickly.

Answer:

The Office of Infrastructure Protection (IP) has made significant progress in the identification, prioritization, and protection of critical infrastructures and key assets.

a) IP has planned for and conducted risk and vulnerability assessments at multiple levels and within/across sectors. IP examines and addresses vulnerabilities across the nation's infrastructure by using a five-step risk management methodology that measures the national risk profile in the context, and absence, of threat information. The major steps of the risk management methodology include:

- Identifying critical infrastructure
- Assessing vulnerabilities
- Normalizing, analyzing, and prioritizing protective measures
- Implementing protective programs
- Measuring effectiveness through performance metrics

The threat environment is dynamic. IP uses this methodology across and within sectors so that when credible and actionable threat information is known, the Office can assess the sector-specific and cross-sector impacts using existing vulnerability assessment information. This allows IP to quickly prioritize protective measures across and within sectors, and implement these measures quickly to reduce the overall risk posed by the threat.

The National Infrastructure Protection Plan (NIPP), as directed by HSPD-7, outlines the roles and responsibilities of the Department, other federal departments and agencies, state and local entities, and the private sector. This comprehensive plan will be completed this year, but efforts are already well underway using the risk management framework previously described to assess vulnerabilities within and across sectors, including in response to specific threats and as part of programmatic activities.

The IAIP Directorate conducts risk assessments every time the Secretary elevates the threat level and IP has shared such assessments with states and local entities to provide guidance on setting priorities for protective measures. IP also conducted an assessment of CI/KR in response to the Congressional requirement to allocate grant funding based in part on identified threats and vulnerabilities as part of the ODP's Urban Area Security Initiative (UASI) grant program.

Additionally, IP assessments are conducted for CI/KR in two primary ways: 1) Site Assistance Visits (SAVs) conducted by IP personnel and 2) as part of the buffer zone protection plans conducted by state and local law enforcement officials. These two methods are conducted strategically and in response to specific threats to identify and mitigate vulnerabilities.

SAVs, focusing inside the fence, facilitate vulnerability identification and mitigation option

discussions. SAVs are conducted by IP security experts in collaboration with owners/operators, security planers, and local law enforcement officials. To date, over 150 SAVs have been conducted across the country in FY04. In addition to providing specific information regarding CI/KR, information derived from SAVs is used to develop two sets of sector-specific reports: *Common Characteristics and Vulnerabilities* (CCV) reports and *Potential Indicators of Terrorist Activities* (PITA) reports. These reports are disseminated to owners/operators and law enforcement officials as tools in their own risk management processes. Determining commonalities within and across sectors allows IP to prioritize assessment and mitigation activities. This is further added to by buffer zone protection plans.

Buffer zone protection plans, a community-based planning process, are designed to identify site-specific vulnerabilities, describe the types of terrorist tactics and activities that likely would be successful in exploiting those vulnerabilities, and implement preemptive and protective actions to mitigate vulnerabilities so that terrorists are no longer able to successfully exploit them. They concentrate on identifying and mitigating vulnerabilities outside the fence line of the facility in the communities surrounding the CI/KR. A vulnerability assessment is part of the planning process and over 800 BZPPs are expected to be implemented this year.

24. A GAO report released last year (GAO-03-439) notes that chemical facilities may be attractive targets for terrorists and that the release of certain chemicals can pose a grave threat to the surrounding population. Despite these concerns, the Administration has opposed mandatory security improvements for the chemical industry. What specific evidence do you have that the industry will voluntarily implement the kind of steps necessary to keep the American people safe?

Answer: We are assisting state and local authorities, as well as private industry, in developing Buffer Zone Protection Plans (BZPPs) for areas immediately adjacent to the "fence line" of critical infrastructure. The approximately 800 BZPPs completed by the end of FY 2004 included roughly 320 chemical sites warranting special attention. For FY 2004 we allocated up to $50,000 per CI/KA site for vulnerability reduction. A data call is currently underway to support the identification of sites for attention in FY 2005 and the Office of Infrastructure Protection (IP) is excepting to complete roughly 2,000 BZPPs next year.

DHS also has established a protection, training, and planning program for state homeland security personnel, local law enforcement, chemical facility operators and site security personnel. Periodic drills among the protective community will be conducted to exercise chemical facilities' response plans in case of a terrorist attack. IP will continue to work with the Office for Domestic Preparedness to incorporate chemical plant security into national exercises.

We are also in the process of hiring Protective Security Advisors (PSAs). Each PSA will have responsibility for a specific region of the county and will maintain a close relationship with the chemical plant owners and operations in their specific area of responsibility. PSAs will facilitate information sharing, organize protective security training, assist in emergency coordination, and represent DHS in the communities in which they are posted.

The activities described above in FY 2004 and continued in FY 2005 will not only greatly increase chemical site security and across all other sectors, but will increase our nation's general protective capacity.

Plum Island

25. The DHS "Budget in Brief" describes an increase of $12.9 million to begin to address the highest priority activities required at the Plum Island Animal Disease Center (PIADC). DHS goes on to explain that these activities "have been validated by internal and external assessments that included as part of the FY2003 General Accounting Office report Combating Terrorism—Actions Needed to Improve Security at Plum Island Animal Disease Center; Report Number GAO-03-847, as well as the deficiencies identified by local and nationally elected officials." On October 29, 2003,following the release of this GAO report, I wrote to Under Secretary Charles E. McQueary asking him to provide a detailed response to the individual issues raised by GAO including schedules for when these issues would be addressed. Dr. McQueary never responded to this request. Consequently, I am now requesting that you respond to the following issues raised by GAO:

With regard to GAO Recommendation #1 concerning the need to correct physical security deficiencies, Dr. McQueary stated in his comments to GAO that DHS conducted a detailed assessment of the facility operations and infrastructure and that the "next steps are to develop a step-by-step corrective action report with timelines and actionable items."

a) Please provide the "step-by-step corrective action report with timelines and actionable items.
b) For each item, identify the funding being requested to address the item.
c) In the interim, what compensatory security measures are being taken to address the security risk created by these deficiencies?

Answer (a) and (b): The first security project, "MOD-2," was based on the threat assessment and recommendations provided by Sandia National Laboratories. This project provides intrusion detection and CCTV cameras for the BSL-3 laboratory perimeter doors and was completed in January 2004.

The next project, known as Phase I, "Compartmentalization," provides physical barriers, (access control, intrusion detection, CCTV, etc.,) which serve to separate the general-access areas of the laboratory from the pathogen-accessible areas. The project began on February 17, 2004. The cost for this project is $1.3 million and the estimated completion date is September 30, 2004.

The next Phase I project (Freezer Security) concerns access control and entry recording to the existing freezer security. We are implementing an internal facility mandate to maintain the pathogens within freezers secured with magnetic locks and balance switches. The freezers can only be accessed by authorized persons using proximity cards and unique personal identification numbers. The security package for each freezer will communicate back to the Security Control Center and will activate alarms and CCTV devices during unauthorized entry incidents,

providing an audit trail of those who have accessed the freezer and video recordings of those entries. This project has an estimated commencement date of August 2004 and a completion date of November 2004. The estimated cost for this project is $125,000.

Phase II (Critical Operation Protection) will enhance the physical security at each area designated as a Critical Operations Area by installing access control, intrusion detection, CCTV devices and physical barriers (fencing). This project has an estimated commencement date of November 2004 and a completion date of June 2005. The estimated cost for this project is $1.75 million and is included in the FY 2005 budget request.

The next project, Phase III (Bio-Containment Compound Perimeter Fencing, New Firehouse, New Emergency Operations Center) will provide the Bio-Containment Compound with a new security fence equipped with detection devices. The fence will be separated into operational zones, covered by CCTV cameras. This project also provides access control, intrusion detection, and CCTV devices for the new firehouse and Emergency Operations Center. This project has an estimated commencement date of November 2005 and a completion date of September 2006. The estimated cost for this project is $3.5 million and is included in the FY 2005 budget request.

Answer (c) In the interim, we have increased the number of armed security officers on the Island from three to six. Further increases are put in place in reaction to elevated terrorism threat level. The added officers are actively patrolling the Island in greater numbers and frequency. We have added a foot patrol within the bio-containment compound. We have more clearly specified the assigned responsibilities to each post for both routine and emergency operations.

Until the physical controls of the Compartmentalization project are completed, all persons entering into the Bio-Containment are considered to have to possibility of entering into the vicinity of the designated "Select Agents" and are thus required to have the background investigations and registration required for that access.

26. With regard to GAO Recommendation #2 concerning the need to limit access to pathogens, Dr. McQueary stated in his response to GAO that DHS has undertaken a detailed study of all existing security-related policies and procedures, "specifically those that relate to the restriction of access to the biocontainment areas." He also stated that DHS plans to develop a "limited use policy to identify access control requirements for all personnel to enter the biocontainment facility." Given the myriad of problems GAO identified concerning limiting access – ranging from open physical architecture and layout of the biocontainment facility to the lack of clear guidelines and adherence to security clearance and escort protocols – it is not apparent that this problem can be adequately addressed by the course of action he proposed.

a) When will the limited use policy described be complete?
b) When will the accompanying access control requirements be in place?
c) How will these ensure that the problems identified by GAO concerning access to pathogens at the facility are fully addressed?

Answer (a): The limited use/access policy is in place now. Limiting access to pathogens involves the control of personnel entering the biocontainment facility, the freedom of personnel to move about in the facility, and the physical constraints controlling access and movement within the facility. Strict entry and exit rules have been put into effect and are controlling access to the facility. Only personnel with approved background clearances may enter the facility unescorted. A strictly enforced and monitored line-of-sight escort policy is fully in effect for any personnel who have a need to enter the facility but have not been cleared through security checks. Contractors working within the biocontainment area are restricted to their work areas by their escort.

Answer (b) The additional access control requirements, their timeline and cost were outlined in the response to Q01098 above.

Answer (c) When all corrective actions are completed, the modifications will address each of the specifics pointed out by the GAO in terms of limiting access to those with a defined need to access, preventing the unauthorized removal of objects from the containment area, eliminating perimeter vulnerabilities to unauthorized access, and maintaining electronic records of accesses and activities within containment. Personnel suitability screening, national background checks and investigations, combined with physical barriers, need- and authorization-based access control, and regular, random searches provide appropriately graded protection.

27. With regard to GAO Recommendation #3 concerning the need to consult with other laboratories to mitigate the inherent difficulty of securing pathogens, Dr. McQueary's response to GAO stated that DHS is working with the Energy Department's National Nuclear Security Administration (NNSA) laboratories, the U.S. Army Medical Research Institute of Infectious Diseases and the National Institutes of Health. It is not clear from his response how, exactly, DHS is consulting with these other government entities to address the problem of securing access to pathogens either at PIADC or generally. It is also not clear that the other agencies being consulted have adequate controls upon which to base such efforts. For instance, in December 2002, the Energy Department Inspector General issued a report critical of the access given to foreign nationals to two Energy Department laboratories, including one managed by NNSA. How is DHS coordinating with other Federal agencies to ensure that access to pathogens is controlled not only at PIADC, but also across the Federal complex?

Answer: DHS biosecurity science and technology programs have the benefit of being staffed by individuals whose experience includes leadership positions in other relevant federal agencies. Among them are individuals who formerly served in leadership positions and as bench scientists at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID), a career Public Health Service officer from the Food and Drug Administration (FDA), a Naval officer and scientist having over a decade of leadership in federal microbial forensic analyses, and a safety specialist from the National Nuclear Security Administration.

Our staff regularly participates in interagency working groups with representatives from the Departments of Defense, Health and Human Services (DHHS) and Agriculture (USDA). Such working groups are an effective instrument for coordinating biosecurity programs. Each of these departments is, for example, represented on the Board of Directors for the National Interagency

Biodefense Campus at Fort Detrick that coordinates biosecurity programs and infrastructure matters on that campus.

DHHS and USDA have the statutory responsibility for regulating access to pathogens across the Federal complex, and DHS operations are compliant with those Departments' responsibilities.

28. With regard to GAO Recommendation #4 concerning the need to enhance incident response capability at Plum Island, your response states that DHS is working with the Federal Protective Service (FPS) to "develop a task for specific assistance to the island." Dr. McQueary's response also stated that funds have been requested to increase the guard force beginning in FY2004. He also stated that the DHS assessment of the facility identified the lack of an incident response plan and that the corrective action plan would, in turn, "identify in detail the path forward in developing this plan." He did not, however, indicate when such a plan would be completed.

a) When will the incident response plan be completed?

b) Dr. McQueary's response did not explain how or when DHS would resolve the issue of the lack of legal authority and policies and procedures for the security force to carry firearms, to make arrests, or to use force. When will these legal and policy issues be resolved? If it has been resolved, how has this matter been concluded?

c) What actions are being taken in the interim to ensure adequate security in prior to these new measures being put in place?

d) When will additional guards actually be in place and how will DHS determine the number of additional guards necessary to secure the facility?

Answer (a) and (b): An incident response plan is currently in place. DHS is working closely with the Federal Protective Service (FPS) to secure the needed federal law enforcement presence that local governments consider imperative on the Island in order to establish mutual aid agreements. FPS placed police officers on site June 2004. PIADC and local governments now execute cooperative agreements regarding emergency response, training exercises, backup assistance, intelligence sharing, and threat assessment. FPS presence also provides the required Federal arrest and detention authority to PIADC, thereby addressing the use of force issue. FPS is finalizing the Building Security Assessment (BSA) to determine the security counter-measures and law enforcement resources that are necessary to secure the facility. FPS has also been asked to consolidate multiple assessments that have been conducted over the past two years.

Answer (c) Actions undertaken to ensure the safety of the facility are outlined in responses to questions 25 and 26 above.

Answer (d) As stated in response to question 25, the number of armed security guards on the Island has been increased to six. That number will be raised to eight once requisite background investigations on prospective employees have been completed. The number of security

personnel is determined by threat assessments. Threat assessments are tools that determine the likely threats that security forces will need to face and this information is used to determine the required number of security personnel. Threat assessments are on-going and we will continue to evaluate and adjust the number of armed security guards as necessary.

29. With regard to GAO Recommendation #5 that DHS reconsider the security risks at PIADC, Dr. McQueary's response indicated that DHS is conducting a review of the "entire security posture of the island again [sic] like facilities" and will issue a revised threat assessment early next year. Measuring PIADC against other similar facilities may not provide an adequate baseline for protection, since we have no assurance, in the aftermath of the September 11 attacks, that these other facilities have adequate levels of security. Please describe how DHS will evaluate the threat against Plum Island and similar biosafety level 3 and 4 facilities?

Answer: DHS, Federal Bureau of Investigation (FBI) and FPS personnel conducted a threat assessment in February 2004. Their report has not yet been received. When the report is received, recommendations will be evaluated and acted upon accordingly. Ensuring the security of the facilities and the people who work in them is an on-going process. As is being done with PIADC, future DHS BSL-3 and BSL-4 facilities will undergo continuous threat assessments and vulnerability assessments by internal and external security experts, including local, state and federal law enforcement. These assessments will guide facility upgrades or procedural adjustments as necessary.

30. With regard to GAO Recommendation #6 that DHS consult with appropriate state and local law enforcement and intelligence agencies to revisit the threats specific to PIADC, Dr. McQueary's response stated that your Department will work with local and national law enforcement in developing a complete set of possible threats for the island. His response did not include any mention of either the Terrorist Threat Integration Center or any intelligence agency.

a) Is DHS consulting with either TTIC or any intelligence agency with regard to its evaluation of risks specific to Plum Island?

b) Is DHS consulting with these intelligence entities with regard to any threats against other similar biosafety level 3 and 4 facilities?

Answer (a) and (b) Intelligence activities are coordinated through DHS's Information Analysis and Infrastructure Protection (IAIP) Directorate. As stated above, threat assessments to the PIADC are a responsibility of DHS security and law enforcement, as well as other law enforcement agencies. The IAIP Directorate, working with the Intelligence Community, will provide any intelligence information related to threats against either PIADC or similar biosafety level facilities.

31. With regard to GAO Recommendation #7 that DHS revise the security and incident response plans to reflect redefined risks, threats, and assets, Dr. McQueary's response stated that DHS has been reviewing these issues and that DHS "will continue to work with other research facilities in developing the islands' threat statement and the security posture required." In response to recommendation #5, he stated that the revised threat assessment would be issued early in 2004.

What is the timetable for revising the security and incident response plans to respond to this revised threat assessment?

Answer: This question is addressed above in response to question 29.

Coast Guard Research and Development Center

32. The FY05 Budget request includes $13.5 million for operations and maintenance of the Coast Guard Research and development Center, although those funds will now be provided through the Science and technology Directorate rather than the Coast Guard budget. However, the budget does not include a specified amount for program activities at the Center. Please describe how the new arrangement will affect operations at the Center and state what the expected funding level for programs at the Center will be during FY05. Also, will the Center continue to address research and development related to all of the Coast Guard's missions, including homeland security and such traditional missions as search and rescue or environmental cleanup?

Answer: The Science and Technology Directorate (S&T) and Coast Guard (CG) are preparing a formal reimbursable agreement that will detail the coordination and funding mechanisms for CG R&D capabilities. The foundation for that agreement is the consolidation of funding requested in the FY2005 budget. For FY 2005, the CG R&D center facility, personnel and maintenance expenses will be funded through S&T in the amount of $13.5 million. In addition, S&T and the CG have agreed upon a base level of additional project funding in the amount of $5 million that will be specifically targeted toward non-security related projects including maritime science and research. This funding will be designed to support CG mission-programs such as Marine Environmental Protection, Living Marine Resources, Search and Rescue, Aids to Navigation and Marine Safety. The specific projects in support of these mission-programs will be prepared annually for S&T concurrence.
In addition to this $18.5 million in funding, the Coast Guard will submit security-related research requests through S&T for coordination across all portfolios and DHS components. The Coast Guard has submitted a maritime security R&D portfolio detailing approximately $50 million in vital maritime security research initiatives. This portfolio has been validated by S&T portfolio managers and will be considered in the development of future spending priorities and commitments from S&T.

This integration of funding and effort will go far to minimize redundancy and maximize the effectiveness of Coast Guard R&D while ensuring that all Coast Guard mission requirements remain a key part of S&T planning and resource decisions.

Human Resources

32. The proposed budget includes well over $100,000 for implementing a new human resources management system (HRMS), intended to be mission-centered, fair, effective, and flexible.

a) The proposed budget states that the HRMS will include a performance-based pay system. To what extent will management officials exercise discretion in deciding individual employees' pay and benefits? To what extent will those decisions be guided or determined by applicable guidelines?

Answer: The proposed regulations provide that pay increases will be based on employee performance. The discretion to evaluate employees is appropriately left to the supervisors and managers who are familiar with the employees' accomplishments. The department will be developing performance management guidance for this process. The proposed regulations do provide for Performance Review Board(s) to oversee the process and ensure fairness and consistency of evaluations. The determination of actual pay-outs will not be left to the discretion of the supervisors and managers but will be a calculation based on the size of the pay pool and the distribution of ratings among employees in the pool.

b) What efforts will be undertaken, and what mechanisms and procedures will be in place, to assure that management officials do not arbitrarily use the system to unfairly advance, demote, or increase or decrease the pay of employees? What resources are identified in the budget for establishing mechanisms and procedures? Please include in your answer a discussion of the development and implementation of performance management systems, competency assessment systems, the training of supervisory personnel to administer the new system, the education of rank-and-file employees regarding the new system, and any other relevant efforts.

Answer: The proposed regulations provide for Performance Review Board(s) to oversee the performance management system to ensure fairness and consistency of evaluations. The FY05 budget request includes $2.5 million for a pay-for-performance system, $42 million for the design and implementation of a pay-for-performance system and for the administration and staffing of the new labor management and appeal process, $31 million for training employees to implement a new pay-for-performance system, and $27 million for program management. The funding for developing the pay for performance system will ensure that the new system will adequately distinguish between performance and acknowledge the importance of competencies in assessing that performance. The funding for training is intended to provide overall training for the proposed system as well as targeted training for managers, supervisors and employees in the application of the new performance management system.

c) What safeguards will be put in place to assure that the levels of pay under the HRMS are sufficient to recruit and retain a high-quality workforce, notwithstanding the competing budget priorities that the Department and its subdivisions will inevitably face?

Answer: The proposal is specifically designed to ensure that the Department remains competitive in recruiting and retaining a high-quality workforce. In addition to a closer link to local markets, pay will be based on the performance of individuals, teams and organizations.

d) What safeguards will be provided to assure that any review panels established under the HRMS to assume responsibilities of the Merit Systems Protection Board (MSPB) and the Federal Labor Relations Authority will be truly independent, expert, impartial, and balanced?

Answer: The proposed HRMS retains the Merit Systems Protection Board (MSPB) for appeals of most conduct and performance issues. There will be a limited number of mandatory removal penalties which will be appealed to a DHS Panel. The processes and standards for appeals will be similar to those existing for MSPB including right of notice, full evidentiary hearings before an adjudicating official, and right of appeal to the DHS Panel. DHS Panel members will be appointed by the Secretary for fixed terms and can be removed only for inefficiency, neglect of duty, or malfeasance (the same standards that apply to the MSPB). Likewise, in proposing the establishment of the DHS Labor Board, the members will be appointed by the Secretary for fixed terms and can only be removed for inefficiency, neglect of duty, or malfeasance. Membership will include one individual from the FLRA; and members cannot be current DHS employees.

e) How will the HRMS protect the right of employees to bargain collectively, and participate through labor organizations of their own choosing in decisions that affect them?

Answer: The proposed regulations specifically ensure the right of employees to organize, bargain collectively, and participate through labor organizations of their own choosing. The proposal leaves intact many of the definitions associated with labor relations including "exclusive representative," "collective bargaining," and "labor organization."

f) How will any mechanism established in the HRMS for appealing personnel actions – *(i)* protect the right of an employee to appeal to the EEOC when an alleged basis for a disputed personnel action is unlawful discrimination within EEOC's jurisdiction; and *(ii)* protect the right of an employee and the power of the Special Counsel to appeal to the MSPB when an alleged basis for a disputed personnel action is retaliation for whistle blowing or other prohibited personnel practices?

Answer: We have proposed to retain the current statutory provisions dealing with mixed cases, i.e. cases involving allegations of discrimination which are also appealable to the MSPB. In addition, we propose that the Department's action will not be sustained if MSPB (as is currently the case) determines that the decision was based on any prohibited personnel practice.

33. What processes will be established for evaluating the new performance management policies and systems in the HRMS, including the safeguards against arbitrary action discussed in the foregoing question, both before they are implemented to be sure they are effective and after they are implemented to assess their performance? What resources are identified in the budget for such evaluation?

Answer: We have built into the FY 2005 request funds to design evaluations of each of the new processes and procedures. Those evaluations will test the effectiveness of the new HRMS, and will be part of an on-going process to ensure that the system meets the needs of the Department while allowing us to attract and retain highly talented and motivated employees.

34. The budget indicates that the new HRMS will be rolled out in phases. What is the anticipated schedule for applying various parts of the new HRMS to particular offices and entities at the Department? On what basis will decisions be made to further define or alter this schedule? Will DHS evaluate and verify particular systems (such as those for assessing skills and competencies, or for analyzing market pay) before they are implemented? Likewise, will DHS evaluate early-implemented parts of the HRMS to assure that they are functioning well before the HRMS is applied more widely?

Answer: The anticipated schedule as proposed in the preamble to the regulations, would have the policies on labor relations, adverse actions and appeals go into effect across DHS no sooner than 30 days following the issuance of the final regulations. In the areas of pay, performance, and classification, the proposal is to implement these changes in DHS Headquarters, IAIP, S&T, and USCG later in calendar year 2004 and early in calendar year 2005. The balance of the covered organizations would be phased in during late calendar 2005 and early calendar year 2006. This implementation schedule is dependent on finalizing the proposals this summer and funding (as requested in the President's FY 2005 budget) for the design and training necessary to ensure the success of this system. The plan is to model and evaluate as many components of the system as possible before implementing them, and to conduct consistent evaluations throughout the implementation to ensure that the design functions as intended. The results of these evaluations will influence the content and schedule of subsequent implementation.

Postal Security

35. The Postal Service has begun deploying sensors in its mail processing facilities that can detect the presence of biological agents, such as anthrax, that are transmitted through the mail. These sensors will allow the earlier detection of these threats, so that the spread of contaminants

can be prevented and suspect mail identified quickly. As you know, the discovery of ricin in Senator Frist's mailroom represents the third recent instance in which it appears that this deadly chemical may have been sent through the mail. The sensors being deployed by the Postal Service can be modified to also detect the presence of harmful chemical agents sent through the mail. The FY05 Budget does not include any funding to support these anti-terrorism efforts. Do you support providing funding to help defray these costs?

Answer: The Science and Technology Directorate recognizes the serious and continuing nature of these threats to the USPS, its employees and customers. The improvement of biosensors for USPS was considered by our Biological Countermeasures Integrated Product Team, and given the state of progress at the time, deferred for this year. It will certainly be considered in all future prioritizations for research funding.

HSARPA is supporting, although indirectly, the development of toxin sensors for USPS. In response to its first research announcement, a contractor currently developing sensors for USPS proposed to modify its USPS sensor as an upgrade to the BioWatch system. HSARPA selected this bid, funded it, and it is now underway. If there were to be additional research performed for modification of USPS sensors to detect toxins, the preferred, most expeditious path would be to accelerate this contractor's work for BioWatch, and then develop/test it for the specific postal applications which are very different from BioWatch.

DHS S&T research portfolios are fully subscribed and carefully prioritized to alleviate the most serious threats with the most devastating consequences to the largest number of people, or economic impact.

Homeland Security Advanced Research Projects Agency

36. The Homeland Security Act of 2002 established the Homeland Security Advanced Research Projects Agency (HSARPA) within the S&T Directorate to be similar in purpose, powers, and organization to the Defense Advanced Research Projects Agency (DARPA) within the Department of Defense. DARPA's success has been grounded in its independent role, which has enabled it to recruit outstanding scientific and technical talent, to promote creativity and adaptability under a lean, flexible organizational structure, to use highly flexible contracting authority, and to entice collaboration from other research and development (R&D) entities by leveraging a large independent source of funds. Unfortunately, as the S & T Directorate has taken shape over the last year, it is clear that HSARPA is not being given sufficient independence and resources to play the role envisioned by the authorizing legislation. Specifically, it appears that portfolio managers from the Plans, Programs and Budgets (PPB) office within the S&T Directorate (which was not contemplated in the statute) control virtually all investment and spending decisions including, for all practical purposes, funding decisions for HSARPA. In addition, the funding level for HSARPA appears far below what was authorized ($500 M for the first fiscal year) and what Congress understood would be available from appropriations for FY2004. Although the Department has testified that the funding level for HSARPA would be $350 M for FY2004, it now appears that the actual amounts the Directorate is now considering will be well below that level.

These problems will severely undermine the ability of HSARPA and therefore the Directorate to execute their missions.
Please answer the following questions:

a) What are the exact funding levels that will be spent by HSARPA in FY2004 in each of the approximately 14 portfolio program areas? What are the projected levels for HSARPA expenditures in each portfolio area for FY 05?

Answer: The Plans, Programs and Budget Office is responsible for gathering and defining scientific and technical requirements for the Department. Funding, and the allocation of that funding to the executing offices (Office of Research and Development, HSARPA, and Systems Engineering and Development) is determined through an Integrated Product Team (IPT) process. The IPT's consist of at least one member from each of the executing offices and the funding decision and funds allocations are made through IPT consensus. Once allocated to an executing office (e.g. HSARPA) that office makes all the decisions about which specific projects are initiated to meet the programmatic requirements as well as who performs the work.

The Homeland Security Advanced Research Projects Agency (HSARPA) has $ 318,685,000 allocated from the FY 2005 President's budget. The table below lists the comparable FY 2004 funding allocation and the FY 2005 funding allocation by the 14 structured portfolios to be executed by HSARPA.

Portfolio	FY 2004 Allocation by Portfolio(in millions)	FY 2005 Allocation by Portfolio(in millions)
Bio Countermeasures	18.37	86.396
Border and Transportation Security	8.646	22.056
Chemical Countermeasures	39.358	36.694
Comparative Studies	0	0
Critical Infrastructure Protection	5.28	4.444
Cyber	17.325	17.500
Emerging Threats	14.74	4.444
Emergency Preparedness & Response	4.84	5.830
High Explosives Countermeasures	6.16	4.306
Radiological/Nuclear Countermeasures	65.56	43.333
Rapid Prototyping	72.16	63.194
Standards	2.2	0
TVTA	13.64	5.556
US Secret Service	1.815	1.944

Portfolio TOTAL	270.094	295.697
SBIR *	19.609	22.988
TOTAL	289.703	318.685

*SBIR funds are drawn from across the various portfolios.

b) Why is HSARPA entirely controlled by PPB and not allowed to effectively participate in either requirements development or DHS S&T R&D budget or funding decisions? How is that consistent with Congressional authorization to stand up HSARPA as a DARPA-like independent entity under the Undersecretary?

Answer: The Office of Plans, Programs and Budgets (PPB) manages and executes the Planning, Programming and Budgeting System (PPBS) cycle for the Directorate, and sets short-, mid-, and long-range goals aimed at achieving the needs set out by the Administration. These goals include, for example, countering the threat of weapons of mass destruction and addressing the needs of customers in the operational Directorates in the Department and of state and local entities. Addressing these goals requires an orderly planning, programming, and budgeting process, which is executed within PPB for the Under Secretary for Science and Technology.

It is important to note that leadership from all of our executing Offices, including HSARPA, participates actively in the PPB process through a set of integrated product teams that are integral to the planning process. The executing Offices then respond to the prioritization process with programs that are subsequently executed.

The analogy between DARPA and HSARPA is at best a weak one. DARPA exists within the Department of Defense as a means for performing undirected research and development — that is, research and development that is not initiated and directed in pursuit of an explicit customer need. Most of the research and development activities within the Department of Defense are in fact directed, and are performed within the acquisition chains of the respective military Service, or at places like the Missile Defense Agency or the Defense Threat Reduction Agency, in pursuit of specific needs.

Within the Department of Homeland Security, however, there are no "Service" research and development entities that span the space of activities required by the President's National Strategy for Homeland Security, or the responsibilities associated with Sec. 302 of the Homeland Security Act. Thus, HSARPA is the primary means for procuring research and development from the private sector, including activities that are driven by customer requirements.

Not all private sector R&D is, however, procured through HSARPA. For example, there are programs where the key issue is not technical—the need to invent some new capability—but rather the need to impose a disciplined systems engineering process in order to deliver the capability in a timely and efficient manner. Those efforts (e.g. counter-MANPADS) reside within the Systems Engineering and Development office. In addition, capital investments, such as the planned National Biodefense and Countermeasures Center (NBACC) facility at Ft. Detrick, are not executed through HSARPA. Finally, private sector investments made through another government agency (e.g. standards work through the National Institute of Standards and

Technology) may be, but are not always, executed most efficiently through HSARPA.)

In addition, it was recognized early that, despite the need for HSARPA to execute requirements-driven programs, a true "DARPA-like" function also needed to be performed. Thus, there is an Emerging Threats budget line that is primarily for the use of the Director, HSARPA, to develop and execute programs that are explicitly not requirements-driven. The role of PPB in that area is simply to set overarching policy, to periodically review the efforts for technical soundness and relevance to the needs of homeland security, and to oversee budget execution. If HSARPA were to become truly "DARPA-like" in character, then another organization would need to be created to execute within the private sector the needs-driven R&D of the Department. This function is where the large majority of private sector funding would reside (as with DoD), and the remaining (non-requirements driven) HSARPA would be quite small.

c) What is the current staffing level for HSARPA, including both full-time and contract employees? What is the anticipated staffing level of HSARPA and by what date will this be reached? What is the current staffing for PPB? Please include information on PPB portfolio managers and whether they are full-time, contract or Intergovernmental Personnel Act (IPA) employees, and what organizations or agencies they come from.

Answer: The current staffing level for HSARPA is 33 FTE's. The staffing plan authorizes 68 FTE's and it is expected that HSARPA will be at full strength before September 30, 2004. The current staffing level for PPB is 84 FTE's. The staffing plan authorizes 104 FTE's. The information on PPB portfolio managers is as follows:

a. 2 full-time IPA's from Sandia National Laboratories covering three portfolios
b. 1 full-time IPA from Pacific Northwest National Laboratory managing two portfolios
c. 2 full-time IPA's from Lawrence Livermore National Laboratory
d. 1 full-time IPA from the Institute for Defense Analysis
e. 6 full time Federal employees

37. I am also concerned that PPB appears to be funneling in excess of $150 million in FY2004 funds, a very large portion of the total R&D funds available, to DOE laboratories, through a two-tiered system of "intramural" and "extramural" DOE labs, such that the "intramural" labs do not compete for their funding. In the authorizing legislation, Congress, with bipartisan unanimity, specifically rejected the model of using an established federal lab as the R&D entity for the Directorate and instead chose a more creative, fast-moving and flexible model represented by HSARPA. HSARPA was created by Congress to focus funding on private, public and academic sector R&D in a highly competitive effort to explore the best new technology options and to promote rapid technology transfer and rapid technology development. Federal laboratory programs were intended to compete as part of that process, not have a guaranteed stream of funding.

For FY 04, how much money will flow from S&T to the DOE labs on a non-competitive basis? What is the comparable, projected figure for FY 05?

Answer: All work performed by Department of Energy (DOE) laboratories for DHS mission related programs is based on first determining that they, in fact, are the best qualified to perform a specific scope of work. The laboratories have done self assessments to identify their best capabilities and have competed on their institutional capabilities. All DOE projects are evaluated on performance based on technical competency, mission and user relevancy, and management effectiveness. The DOE laboratories are projected to get approximately $200M in FY 2004 funding. At this time, there is no projected funding amount that will go to the DOE laboratories in FY 2005.

b) Please explain the process by which certain laboratories were selected to be included in the "intramural" list of labs.

Answer: The research, development, testing, and evaluation capabilities needed to support the missions of the Department of Homeland Security are being defined and institutionalized within the Department. Support of those needs now and in the future requires the establishment and support of an enduring capability that includes scientists and engineers who are well-versed in the requirements and technologies associated with homeland security, and dedicated to the mission of the Department, as well as physical facilities that support their efforts. The legislation creating the Department of Homeland Security and the Science and Technology Directorate recognized that many of these needed capabilities exist within the Department of Energy's (DOE's) laboratories and sites and provided for access to them in support of the Department's mission.

Certain of the existing DOE laboratories have sufficient critical mass and expertise across multiple disciplines to perform the necessary threat assessments and, thus, to participate in DHS's and the S&T Directorate's internal systems analyses, associated trade studies, and long-range planning that will form the basis for the architectures that are ultimately developed and deployed to secure the homeland. These scientists will be intimately involved in assisting the S&T Directorate in setting research goals and requirements and formulating the research and development roadmaps.

A number of approaches have been explored to enable the most effective and appropriate use of these vital resources. Current law, regulation, and policy allows the DOE laboratories in principle to respond as prime contractors to open non-competitive solicitations to the private sector (e.g. Broad Agency Announcements, or BAAs) and to perform as subcontractors or team members on competitive solicitations. However, the S&T Directorate has always recognized the critical importance of ensuring a "level playing field", and hence the need for guarding against organizational conflicts of interest and inappropriate use of "inside information" for those organizations responding to open solicitations to the private sector. The first mechanism that the S&T Directorate explored to address this concern was the concept of "intramural" and "extramural" laboratories. In this approach, some DOE laboratories would be considered part of the intramural team for planning purpose, and others would be considered extramural. Only extramural labs would be eligible to respond to HSARPA and SED solicitations. This approach

has now been revisited based on the direct feedback from several of the laboratories. However, the need to ensure equity in the process and preclude organizational conflicts of interest remains.

Laboratories that have access to government planning information – and thus in fact are part of the planning process – will not be able to participate in broad agency announcements, or in industrial teaming relationships, such as those solicited by HSARPA or SED. These funding sources currently represent the majority of the funding that the S&T Directorate will spend on developing technologies for DHS. All of the DOE laboratories will be eligible for project funding from S&T's Office of Research and Development, however. In addition, those laboratories that do not contribute to our planning would be able, as the law permits today, to respond to BAAs and to team with industry in response to HSARPA and SED solicitations. The decision as to whether a laboratory wants to be positioned to potentially participate in our planning processes, and hence to be ineligible for HSARPA funding, will be a decision each laboratory will make individually.

Post-Hearing Questions for the Record
Submitted to the Honorable Tom Ridge
From Senator Arlen Specter

"The Department of Homeland Security's Budget Submission for Fiscal Year 2005"

February 9, 2004

During your recent appearance before the Senate Governmental Affairs Committee on February 9, 2004, you addressed the federal government's information sharing efforts. Then, when you appeared before the Appropriations Subcommittee on Homeland Security on February 10, 2004, I asked that you provide an updated assessment on the effectiveness of the federal government's information sharing mechanism, particularly as it relates to our counterterrorism and related efforts. My question is prompted, in part, by the impending one-year anniversary of the formal stand-up of the Terrorist Threat Integration Center (TTIC). At the time TTIC was announced in the January 2003 State of the Union address, I was considering introducing legislation to empower the Secretary of Homeland Security to direct other relevant entities to share intelligence and related information with the Intelligence Analysis and Infrastructure Protection (IAIP) within the Department of Homeland Security. I have to date deferred such action.

Please provide your assessment of all aspects of the proposed improvements to the federal government's information sharing mechanisms, many of which were less than effective prior to September 11, 2001, including but not limited to the effectiveness of new entities *e.g.*, TTIC, Terrorist Screening Center, that were formed subsequent to the passage of the Homeland Security Act of 2002 in order to facilitate better information sharing, among other things.

Answer: Regardless of the particular analytic roles of USG counterterrorism elements (whose roles and interactions are described in detail in Attachment 1), we have committed all such elements, consistent with the President's policies, to share terrorism information (as defined by

the Memorandum of Understanding on Information Sharing, dated March 4, 2003) with one another to ensure a seamless integration of such information.

In answering the question, please address the effectiveness of both "horizontal" sharing *i.e.*, among federal government agencies, and "vertical" sharing, *i.e.*, between federal government agencies and state and local officials.

Answer: Wheras TTIC's terrorism analytic mission is global in nature, IAIP's mission is singularly focused on the protection of the American homeland against terrorist attack. IAIP's singular focus on the homeland allows it to carry out all missions assigned to it by the Homeland Security Act, including the following:

- Facilitating the creation of requirements, on behalf of the Secretary of Homeland Security and DHS leadership, to other DHS components, and to the larger intelligence, law enforcement, and homeland security communities, in order to integrate homeland security information from all sources with vulnerability and risk assessments for critical infrastructure prepared by IAIP; and

- Working with the FBI and others to ensure that homeland security-related intelligence information is shared with others who need it, in the Federal, state, and local governments, as well as in the private sector.

Please refer to Attachments 1 & 2 for additional information.

Also, please clarify the roles of the relevant federal entities in interest concerning the new information sharing mechanisms, *e.g.*, TTIC, IAIP, and the effectiveness of each in light of current statutory, regulatory and other *e.g.*, Director of Central Intelligence (DCID), guidance. Please do so in a manner that incorporates and expands upon your coordinated response to the October 30, 2003, correspondence of Senators Collins and Levin on this topic.

Answer: Please refer to Attachments 1 & 2 for detailed descriptions of the roles and interactions of TTIC, FBI, CTC, and IAIP in light of current statutory, regulatory, and DCID guidance.

Federal Register

Friday,
February 20, 2004

Part IV

Department of Homeland Security

Office of the Secretary

6 CFR Part 29
Procedures for Handling Critical Infrastructure Information; Interim Rule

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 29

RIN 1601–AA14

Procedures for Handling Critical Infrastructure Information; Interim Rule

AGENCY: Office of the Secretary, Department of Homeland Security.

ACTION: Interim rule with request for comments.

SUMMARY: This interim rule establishes procedures to implement section 214 of the Homeland Security Act of 2002 regarding the receipt, care, and storage of critical infrastructure information voluntarily submitted to the Department of Homeland Security. The protection of critical infrastructure reduces the vulnerability of the United States to acts of terrorism. The purpose of this regulation is to encourage private sector entities to share information pertaining to their particular and unique vulnerabilities, as well as those that may be systemic and sector-wide. As part of its responsibilities under the Homeland Security Act of 2002, this information will be analyzed by the Department of Homeland Security to develop a more thorough understanding of the critical infrastructure vulnerabilities of the nation. By offering an opportunity for protection from disclosure under the Freedom of Information Act for information that qualifies under section 214, the Department will assure private sector entities that their information will be safeguarded from abuse by competitors or the open market. In addition, information from individual private sector entities combined with those from other entities, will create a broad perspective from which the Federal government, State and local governments, and individual entities and organizations in the private sector can gain a better understanding of how to design and develop structures and improvements to strengthen and defend those infrastructure vulnerabilities from future attacks.

DATES: This interim rule is effective February 20, 2004. Comments and related material must reach the Department of Homeland Security on or before May 20, 2004.

ADDRESSES: Submit written comments to Janice Pesyna, Office of the General Counsel, Department of Homeland Security, Washington, DC 20528. Electronic comments may be submitted to *cii regcomments@DHS.gov.*

FOR FURTHER INFORMATION CONTACT: Janice Pesyna, Office of the General Counsel, (202) 205–4857, or Fred Herr, Information Analysis and Infrastructure Protection Directorate, (202) 360–3023, not a toll-free call.

SUPPLEMENTARY INFORMATION:

Public Participation and New Request for Comments

The Department of Homeland Security (Department or DHS) encourages the public to participate in this rulemaking by submitting comments and related materials. All comments received will be posted, without change, to the DHS Web site (*http://www.dhs.gov/pcii/*) and will include any personal information provided.

Submitting comments: To submit a comment, please include the full name and address of the person submitting the comment, identify the docket number for this rulemaking, indicate the specific section of this document to which each comment applies, and give the reason for each comment. Comments and supporting material may be submitted by electronic means, mail, or delivery to the Department of Homeland Security, Washington, DC 20328. The Department will consider all comments and material received during the comment period. The Department may change this rule in view of them.

Regulatory History

On April 15, 2003, the Department published a notice of proposed rulemaking entitled "Procedures for Handling Critical Infrastructure Information" in the **Federal Register** (68 FR 18523), 6 CFR part 29, RIN 1601–AA14. As stated in the notice of proposed rulemaking, the Department intended to implement this interim rule as soon as possible. The Department finds that the need to receive critical infrastructure information, as soon as practicable, furnishes good cause for this interim rule to take effect immediately under section 808 of the Congressional Review Act.

For many years, private industry has indicated that its reluctance to share critical infrastructure information with the Federal government is based upon a concern that the information will not be adequately protected from disclosure to the public. Furthermore, private sector entities fear that entities intending to harm our nation, as well as potential business competitors, could seek to use the Freedom of Information Act or other disclosure processes to obtain sensitive or confidential business information not otherwise available to the public. Release of such information could facilitate the efforts of those persons or entities planning or attempting to cause physical or economic harm to our nation or to a particular company or industry.

The responsibilities of the Department include taking action to prevent terrorist attacks within the United States and reducing the vulnerability of the United States to acts of terrorism. The reduction of that vulnerability includes the protection of vital physical or computer-based systems and assets, collectively referred to as "critical infrastructure," the incapacitation or destruction of which would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of these matters.

The Department recognizes the importance of receiving information from those with direct knowledge of the security of that critical infrastructure in order to help reduce our nation's vulnerability to acts of terrorism. The Department believes the voluntary sharing of critical infrastructure information (CII) has been slowed due to concerns that information might be released to the public.

The Department recognizes that its receipt of information pertaining to the security of critical infrastructure, which is not customarily within the public domain, is best encouraged through the assurance that such information will be utilized for securing the United States and will not be disseminated to the general public. Accordingly, section 214 of the Homeland Security Act, subtitle B of title 2, which is referenced as the Critical Infrastructure Information Act of 2002 (CII Act of 2002), directly addressed this problem by establishing a program that protects from disclosure to the general public any CII that is voluntarily provided to the Department. Section 214(f) of the statute provides for fines and imprisonment under title 18 (Crimes and Criminal Procedure) of the United States Code for unauthorized disclosure of CII.

The interim rule will provide the Department with the framework necessary to receive CII and protect it from disclosure to the general public. This interim rule provides flexibility to allow the Department to adapt as program operations evolve. This interim rule sets out a basic set of regulations that implements the Protected CII Program. The Department will continue to consider public comments to this interim rule and determine whether possible supplemental regulations are needed as experience is gained with implementing the CII Act of 2002.

Discussion of Comments and Changes

The Department received 117 different sets of comments on the proposed rule during the initial comment period. The Department has considered all of these 117 sets of comments, and summaries of the comments and the Department's responses follow.

CII and Protected CII

The Department received six comments suggesting the need to make the distinction between CII and Protected CII clearer throughout the rule. This regulation establishes the program for the receipt, handling, use, and storage of a specialized category of information that is voluntarily submitted to the Department and meets the criteria for Protected CII. Not all CII necessarily will be Protected CII. Recognizing that the proposed rule did not in all instances use the terms "CII" and "Protected CII" consistently, the interim rule has been modified throughout where appropriate.

Indirect Submissions

The Department received 20 comments expressing concern regarding the proposed provision that would enable other Federal government entities to act as conduits for submissions of CII to the Department. Comments observed that extending the protections of the CII Act of 2002 to information submitted to agencies other than the Department was outside the authority of the Department. Further, comments highlighted the increased potential for unauthorized use and disclosure of information, as well as the burden that indirect submissions might place on other entities. Comments requested that all references to indirect submissions be removed and that the rule's terms be clarified so that no section could be interpreted to express or imply that material may be submitted to another Federal government agency.

Three comments supported allowing indirect submissions as proposed in the notice of proposed rulemaking; however, these comments, too, highlighted the need for clarification of how such a provision might be implemented and sought additional clarification to ensure that questions regarding the status of CII submitted to an entity other than the Department will be avoided. Support for indirect submissions recognized the Department's original intent, which was to further encourage the sharing of CII with the Federal government. Owners and operators of the nation's critical infrastructures have established relationships with other Federal agencies (*e.g.*, agencies that are sector leads for a particular infrastructure) and are comfortable sharing information with those entities. The Department did not want to impede information sharing and, consequently, our ability to protect our nation, by limiting the ability of submitters to share CII with the Department using those existing relationships.

Recognizing that, at this time, implementation of such a provision would present not only operational but, more importantly, also significant program oversight challenges, the Department has removed references throughout the rule to indirect submissions. Specifically, § 29.1 has been revised to ensure that "receive" is not interpreted to mean that material may be submitted to Federal government entities other than the Department. Section 29.2(i) has been revised to clarify that only the Department and no other Federal government entity shall be the recipient of voluntarily submitted CII. Sections 29.5(a), 29.5(b), and 29.5(c) have been revised to remove references to indirect submissions and to clarify that submissions must be made directly to the Protected CII Program Manager or the Program Manager's designee.

After the Protected CII Program has become operational, however, and pending additional legal and related analyses, the Department anticipates the development of appropriate mechanisms to allow for indirect submissions in the final rule and would welcome comments on appropriate procedures for the implementation of indirect submissions. Comments in support of, or opposed to, the proposed framework for indirect submission of CII to DHS should fully set forth, with relevant citations to the CII Act of 2002 and any other statutory, legislative, or case authorities that may be applicable, the basis for the position they advance.

Relationship Between Protected CII and Other Similar Regulations

The Department received four comments regarding the relationship between this rule and similar Federal agency rules such as the Transportation Security Administration's (TSA) Sensitive Security Information (SSI) rule and the Federal Energy Regulatory Commission's (FERC) Critical Energy Infrastructure Information (CEII) rule. The comments requested that the Department review and clarify the relation of the Department's procedures with similar procedures created by other Federal agencies for the same types of data.

Under certain limited circumstances, there may be information designated as CII under this interim rule that may also constitute SSI under regulations administered by TSA. SSI is information that the Administrator of TSA has determined must be protected from unauthorized disclosure in order to ensure transportation security. The TSA Administrator's authority to designate information as SSI is derived from 49 U.S.C. 114(s).

TSA's regulation implementing this authority, which is set forth at 49 CFR part 1520, specifies certain categories of information that are subject to restrictions on disclosure, both in the hands of certain regulated parties and in the hands of Federal agencies. Currently, the SSI regulation applies primarily to security information related to the aviation sector such as: Security programs and procedures of airport and aircraft operators; procedures TSA uses to perform security screening of airline passengers and baggage; and information detailing vulnerabilities in the aviation system or a facility. SSI is created by airports and aircraft operators and other regulated parties, pursuant to regulatory requirements. TSA also creates SSI, such as screening procedures and certain non-public security directives it issues to regulated parties. The SSI regulation prohibits regulated parties from disseminating SSI, except to those employees, contractors, or agents who have a need to know the information in order to carry out security duties.

Like the provisions of the Homeland Security Act governing CII, TSA's SSI statute and its implementing regulation trigger one of the statutory exemptions to the general disclosure requirements of the Freedom of Information Act (FOIA). *See* 5 U.S.C. 552(b)(3). Thus, both Protected CII and SSI held by the Federal government are exempt from public disclosure under the FOIA. In addition, TSA is currently considering amendments to its SSI regulation that would make it civilly enforceable against employees of DHS and the Department of Transportation, which are the Federal agencies most likely to maintain SSI. In contrast, unauthorized disclosure of Protected CII by a Federal employee is subject to criminal penalties.

Another key difference between SSI and Protected CII is the extent to which a Federal employee may disclose such information. Under TSA's SSI regulation, TSA may disclose SSI to persons with a need to know in order to carry out transportation security duties. This includes persons both within and outside the Federal

government. This rule proposes disclosure of Protected CII to entities that have entered into express written agreements with the Department and, in some cases, requires the written consent of the submitter before disclosure is permitted. Thus, in cases where information qualifies as both SSI and Protected CII, a Federal employee must treat the information according to the stricter disclosure limitations applicable to Protected CII.

In practice, the situations in which information constitutes both SSI and Protected CII may be limited. For the most part, information that is SSI is created by TSA or is required to be submitted to TSA or to another part of the Federal government Therefore, it ordinarily will not be voluntarily submitted, which is a required element for Protected CII designation. In addition, SSI might or might not relate to critical infrastructure assets. Nonetheless, DHS will work to ensure that TSA's SSI regulation identifies any instances in which there may be an overlap between the SSI and Protected CII regulatory schemes and clarifies the applicable requirements for the handling of such information.

Other comments expressed concern regarding the relationship between Protected CII and the rule set forth in the Critical Energy Infrastructure Information program of the Federal Energy Regulatory Commission. These rules are not the same. They operate in a very different fashion with respect to the disclosure requirements of FOIA. On February 21, 2003, FERC promulgated final regulations establishing the CEII procedures, whereby persons with a demonstrated need to know who agree to no further dissemination can be provided with certain information not otherwise available through FOIA. (68 FR 9857 (March 3, 2003)) While information that meets the FERC definition of CEII remains protected from disclosure under existing FOIA exemptions, an alternative means of sharing certain CEII is established, including through a CEII Coordinator charged with verification of the need of requesters for access and the use of non-disclosure agreements via a non-FOIA disclosure track. In other words, the FERC program does not create any exempting authority that would change FOIA disclosure requirements, whereas section 214 of the Homeland Security Act, which is the basis for the Department's CII regulations, does.

Definitions

The Department received several comments regarding terms defined in § 29.2. The following sections address each of the terms in greater detail.

Critical Infrastructure and Protected System

The Department received two comments expressing concern that the terms "critical infrastructure" and "protected system" were not sufficiently defined. The comments suggested that examples be provided and that phrases such as "debilitating impact" be further defined. The Department notes that Congress in the CII Act of 2002 prescribed the definition of "protected system." The Department believes that the definition provides an appropriate degree of flexibility necessary to ensure that information pertaining to the protection of these assets could potentially be shared with the Department.

That said, the Department bases its construction of the regulatory definition on the CII Act of 2002 itself. The Department is mindful that private sector submitters, as the owners and operators of most of the nation's critical infrastructures, are the most well versed as to what information in their particular sector or industry might qualify as CII; therefore, the Department does not wish to unduly restrict the scope of what may be submitted as CII under the Act. As part of its evaluation process in determining whether information meets the criteria for Protected CII, the Department will consider the belief of the submitter that the information merits protection under the Act.

Critical Infrastructure Information

The Department received 11 comments suggesting that the definition of CII be expanded and clarified. Several of the comments wished to expand the definition to include network and topology information for critical infrastructures. The comments also emphasized that expansion of the definition would provide submitters with guidance regarding the type of information that the Department is looking to receive and also ensure that other important information is afforded the protections of the CII Act of 2002, therefore further encouraging submissions. The comments requested that a detailed explanation of "not customarily in the public domain" be provided and encouraged the Department to develop procedures for evaluating whether information is in the public domain. One comment requested that the rule further describe the specific records or information that would be considered by the Department for protection under the CII Act of 2002. Further, comments suggested that the rule specify what information is not CII so that submitters know what types of information should not be submitted. The Department notes that Congress in the CII Act of 2002 prescribed the definition of CII.

The Department believes that the definition provides the appropriate degree of flexibility necessary to further promote information sharing by providing submitters with an opportunity to provide the information they believe meets the definition and should be protected.

The Department also received two comments noting that the proposed rule defined CII as both records and information. Comments suggested that the term "record" be removed from the rule while other comments supported defining CII as both. As a practical matter, these two terms are virtually interchangeable in a context such as this. Accordingly, § 29.2 has been revised to say "CII consists of records including and information concerning * * *"

Voluntary/Voluntarily

The Department received 11 comments regarding the broad definition of "voluntary." The rule defines information that is not voluntarily provided as that information which the Department has exercised legal authority to obtain. The comments expressed concern that this could permit submitters to share with the Department information that is involuntarily collected by other Federal entities. The rule follows the explicit language of the Homeland Security Act and allows for the voluntary submission of information to the Department that is involuntarily collected by other Federal agencies, subject to certain requirements. These restrictions are found throughout the rule, primarily in § 29.3(a), which states that its procedures do not apply to or affect any obligation of any Federal agency to disclose mandatorily submitted information (even where it is identical to information voluntarily submitted pursuant to the CII Act of 2002), and § 29.5(a)(4), which has been added to the rule to address specific concerns raised by commenters. Section 29.5(a)(4) requires submitters to certify that the particular information is being voluntarily provided to the Department; that the information is not being submitted in lieu of independent compliance with a Federal legal requirement; that the information is of a type not customarily in the public domain; and whether the information is required to be submitted to a Federal

agency. If the information is required to be submitted to a Federal agency, the submitter must identify the Federal agency and the legal authority mandating that submission.

Good Faith

The Department received 26 comments requesting that the rule define the term "good faith" and establish procedures for determining that material has been submitted in good faith. Comments also asserted that the proposed rule had the potential to establish a system where material that was not submitted in good faith, and thus does not qualify for protection, would never be made public. Comments suggested that the Protected CII Program Manager should inform submitters when a decision is made that information was not submitted in good faith and provide them with an opportunity to provide an explanation. Other comments recommended deleting references to "good faith" in their entirety.

The Protected CII program is based upon a relationship of trust with the public that the information submitted will be carefully evaluated, marked, and utilized for the purposes of protecting the nation. As recommended by a number of these comments, § 29.5 has been revised, deleting the requirement for the submitters to *certify* that they are submitting the information in good faith. Instead, § 29.5 now provides that the submitters are presumed to have submitted the information in good faith. False representations may constitute a violation of 18 U.S.C. 1001 and are punishable by fines and imprisonment. The intent of such a provision is to provide a remedy to prevent a party from repetitively submitting information in bad faith solely to consume agency resources and from submitting information in an attempt to shield from the public any evidence of wrongdoing.

Independently Obtained Information

The Department received five comments regarding the definition of "independently obtained information." Comments claimed that the proposed definition was not consistent with the CII Act of 2002. In addition, one comment correctly noted that to ensure clarity the provision should be revised to indicate that independently obtained information does not include information that has been directly or indirectly derived from Protected CII. The Department has revised § 29.3(d) to alleviate confusion and ensure consistency with the legislation.

Protected CII Program Management and Administration

Consistent with the CII Act of 2002 and this regulation, the Under Secretary for Information Analysis and Infrastructure Protection (IAIP) is the official responsible for the receipt, safeguarding, storage, handling, and dissemination of Protected CII. The Under Secretary oversees and administers the Protected CII Program. Many comments expressed concern regarding details of the procedural implementation of the Protected CII Program. In addition, other comments recommended that the program begin operations as soon as possible after publication of this interim rule.

To implement this regulation in an efficient manner, the Department intends to use a phased approach that gradually expands the capabilities of the Program to receive submissions. Initially, submissions will be received only by the Protected CII Program Office within the Information Analysis and Infrastructure Directorate (IAIP) of the Department.

Subsequent phases will expand the points of entry for information within the Department. During the initial phase, only paper or electronic submissions (*e.g.*, floppy disks, CDs, etc.) delivered via U.S. Mail, commercial delivery service, courier, facsimile, or hand delivery will be accepted. As the Program evolves, e-mail and oral submissions (*i.e.*, voice mail or person-to-person) will be accepted. The capabilities of the Program to share information that has been validated as Protected CII also will expand. The Department envisions that Federal, State, and local government entities that would like to access and use Protected CII shall enter into an express written agreement with the Department. Such an agreement will outline the responsibilities for handling, using, storing, safeguarding, and disseminating Protected CII; require entities to put in place similar procedures for investigating suspected or actual violations of Protected CII procedures; and establish guidelines for imposing penalty provisions for unauthorized disclosure similar to those identified in the CII Act of 2002 and this regulation. Entities that do not sign such an agreement with the Department will not have access to Protected CII. Initially, the Department intends to share Protected CII only within the IAIP Directorate and with other DHS components, although exceptions may be made on a case-by-case basis. As the Program evolves and agreements with additional entities are finalized, the disclosure of information will expand to other Federal government entities, State, and local government entities, and eventually to foreign governments.

The Department received one comment suggesting that the proposed rule would overburden the Department by creating a situation where only one employee of the Department is responsible for receiving submissions and validating Protected CII. Other comments questioned how the Protected CII Program Manager would have the expertise, resources, and ability to handle the workload that may result from these provisions. The Department does not envision a situation in which only one employee is handling submissions and validating Protected CII. The Under Secretary for IAIP is responsible for directing the Protected CII Program and overseeing its day-to-day operations. In this capacity, the Under Secretary will ensure that the Program Manager or Program Manager's designees consult with other Department officials, as appropriate and necessary, to evaluate the validity of submissions. In addition, a staff and other resources required to perform the responsibilities outlined in the interim rule will support the Protected CII Program Manager. References throughout the rule to the Protected CII Program Manager have been revised to include "or designees", where appropriate, to indicate that other individuals will be designated to handle receipt, validation, and other duties related to the day-to-day operations of the Protected CII Program.

The Department also received three comments requesting that the rule be clarified to specify in greater detail the selection, training, and support of Protected CII Officers. The Department intends to encourage Federal, State, and local (including tribal) government entities that have signed an agreement with the Department to access and use Protected CII to appoint a Protected CII Officer who has been trained and is familiar with procedures for safeguarding, handling, transmitting, and using Protected CII. While this is addressed in greater detail in Protected CII Program procedures, the role of Protected CII Officer may be assigned to an individual in addition to their other duties. The Protected CII Program Manager shall establish procedures outlining the responsibilities of Protected CII Officers and will work with Federal government, and State and local entities in the identification, selection, training, and oversight of Protected CII Officers.

The Department received one comment recommending that

implementing directives discussing how the Protected CII Program will be managed be subject to public review and comment. The Department will follow all provisions of the Administrative Procedure Act in implementing the CII Act of 2002 and this regulation; all policies, and changes to policies, that are required to proceed by way of public notice will do so. Program office development, including but not limited to the Protected Critical Infrastructure Information Management System, used for tracking information voluntarily submitted under the Act, will be consistent with the existing standards of the Department and the Federal government. The Department intends to measure and assess the Program's performance and conduct internal audits to ensure that its goals and objectives are met. The Department recognizes that the success of the Protected CII Program depends on submitters and those with whom Protected CII is shared having an understanding and appreciation of Protected CII Program procedures.

Protected CII Management System

The Department received five comments expressing concerns about the Department's ability to adequately ensure the security of the Protected CII Management Systems (PCIIMS) database. The PCIIMS is a tracking system, not a storage database for the PCII itself. The PCIIMS will be used to track the receipt, acknowledgement, validation, storage, dissemination, and disposition of Protected CII. It is the Department's intent that Protected CII will be maintained in a manner that ensures that it is kept separate from information pertaining to the source of the submission. The Department received two comments requesting that the tracking number be extended to material that has been validated as Protected CII. In addition, one comment recommended that there be a mechanism to track the status of material marked as Protected CII in the event that the status of the information changes. The Department has reviewed this regulation and, consistent with this regulation and these comments, the tracking number assigned to the submission will accompany the material from the time that it is received by the Protected CII Program Manager. The Protected CII Program Manager will establish programs and procedures regarding the security of all Protected CII, including the data stored on the Protected CII Management System (PCIIMS). In addition, the Department will ensure compliance with all appropriate Departmental and Federal government information security policies.

Presumption of Protection

The Department received five comments regarding the presumption of protection afforded to submissions received by the Protected CII Program Manager but for which a final validation determination has not been made. These comments asserted that material does not qualify for protection just because it has been submitted to and received by the Department. The Department also received eight comments encouraging the Department to consider including a time frame for making validation determinations. Comments expressed concern that, combined with the presumption of protection, the lack of a time frame for validating submissions could result in material that does not qualify for protection retaining protection for long periods of time. The Department also received four comments supporting the presumption of protection. These comments noted that absent such a provision submitters would be unlikely to submit CII of a sensitive nature. The Department agrees that in order to promote information sharing the presumption of protection is a necessary provision. The Department agrees that the validation of submitted material must be completed in a timely manner. Submitters, the public, and users of Protected CII within Federal, State, local, and foreign governments must be assured that decisions will be made in a timely manner that allows Protected CII to be used appropriately. Additional language has been added to § 29.6(e)(1), therefore, indicating that the Protected CII Program Manager or designees will review and make a validation determination as soon as practicable following receipt of the submission. The Department considered identifying a more specific time frame; however, the Department does not believe it wise to limit the Program Manager's ability to determine what time frame is feasible given the constraints of program resources and the nature of the submissions received.

The Department also agreed with one of the comments that suggested the proposed language should be revised to read "presumed to be *and* will be treated" (emphasis added for clarification) in § 29.6(b). Section 29.6(b) has been revised accordingly.

Freedom of Information Act Requests

The Department received nine comments requesting that the rule be clarified to explain how FOIA requests will be handled during the period of time in which the Protected CII Program Manager is making a determination regarding whether the submission is Protected CII. Comments further recommended that when a FOIA request is received, the Protected CII status should be reviewed to ensure that the designation remains appropriate. Further, comments requested that submitters be notified when the Department receives a FOIA request concerning the information that they submitted. FOIA requests concerning Protected CII will be handled in accordance with the Department's existing FOIA processes and Executive Order 12600. *See* U.S. Department of Justice, Office of Information and Privacy's Freedom of Information Act Guide & Privacy Act Overview, May 2002 Edition. The Protected CII Program Manager or designees will work closely with the Department's FOIA Officer to handle FOIA requests of Protected CII in a manner consistent with FOIA.

Marking of Information

The Department received two comments highlighting a potential area of confusion regarding marking of materials for protection under the CII Act of 2002. The comments incorrectly asserted that material would be marked with the "express statement" and that the marking would provide direction for the material's handling. It is correct that submitters must include the express statement as identified in § 29.5(a)(3) when material is submitted to the Department; however, that statement is not used in the marking of Protected CII. When such information is validated and has been found to warrant protection under the CII Act of 2002, the Protected CII Program Manager will mark the material with the marking found in § 29.6(c), which makes specific reference to this regulation.

The Department received six comments requesting that the Department include provisions for segregating information so that information that is not protected under the CII Act of 2002 is clearly marked and only information that is absolutely necessary to the protection of the nation's critical infrastructure is kept from public view. The Department does not at this time intend to "portion mark" Protected CII. It is the Department's belief that requiring submitters to "portion mark" material at the time of submission may impede the full disclosure of information. Instead, the Department will consider a submission to be Protected CII as long as it in substance meets all of the requirements for protection. In making validation determinations, the Department will carefully review the

submitted information against the certification by the submitter to ensure that the information is provided voluntarily, in good faith, and is not required by law to be submitted to DHS.

Storage of Protected CII

The Department received seven comments regarding the storage of Protected CII material. Comments expressed concern that the requirements are not sufficient to protect against unauthorized access. For example, the comments noted that a "locked desk" is not generally recognized as a "secure container." In addition, comments suggested that additional safeguards should be considered for information that is aggregated within one facility, area, or system.

In response, § 29.7(b) has been revised to address these concerns about safeguarding Protected CII. In accordance with Federal government requirements for protecting information and information systems, the Department will take proper precautions to ensure that Protected CII is appropriately safeguarded. Furthermore, this section has been revised to clarify how Protected CII should be safeguarded when in the physical possession of a person.

Transmission of Information

The Department received eight comments regarding the treatment of U.S. first class, express, certified, or registered mail and secure electronic means as equivalent means of transmission in terms of the security they provide. Further, comments noted that § 29.7(e) did not allow for use of commercial delivery firms or person-to-person delivery. The comments noted that the proposed rule's specific listing of modes that were acceptable for transmitting information was restrictive. In response, the Department has broadened the language to include any secure means of delivery as determined by the Protected CII Program Manager. This change alleviates any problem of the rule implicitly, but unintentionally, prohibiting other transmission modes that were not included in the list. As technology advances, this language will allow the Department to utilize new transmission modes, as appropriate.

Disclosure of Information

The Department received two comments recommending that any advisories, alerts, and warnings issued to the public should not disclose the source of any voluntarily submitted CII that forms the basis for the warning or information that is proprietary, business sensitive, relates to the submitting person or entity, or is otherwise not appropriately within the public domain. The Department agrees with these comments in significant part. Section 29.8(a) has been modified to include language similar to that contained in the comments.

Twelve comments were received requesting that notification be made to submitters prior to disclosure of their information. Some of the comments also went so far as to request that the prior written consent of the submitter be obtained before Protected CII is disclosed. The comments also suggested that submitters should be made aware of the content of any alerts, advisories, and/or warnings that are issued based on Protected CII. The Department envisions that it will be able to track the disclosure of Protected CII to other Federal government entities and State, and local government entities. In addition, these entities will be asked to track further disclosure of Protected CII within their respective entities. The Department recognizes the desire of submitters to control the release of the information that they submitted; however, such a provision for prior notification has the potential to place a significant administrative burden on the Department. The Department does agree that further disclosure of information beyond those entities or individuals that have entered into a formal agreement with the Department may require the permission of the submitter.

The Department received seven comments regarding disclosure of Protected CII to contractors, each of which encouraged the Department to require contractors to comply with the requirements of this regulation through express written agreements with contractors. The Department received one comment requesting clarification regarding whether State and local governments would be able to share Protected CII with contractors acting on behalf of the Federal government and managing critical infrastructure assets without the submitter authorizing State and local entities to do so. The Department agrees that contractors should be required to comply with the requirements of this regulation. It is the intent of the Department that the Department as well as other Federal, State, and local government entities that access Protected CII shall put in place the necessary written agreements to ensure that the regulations are appropriately adhered to.

The Department received 14 comments regarding the sharing of Protected CII with foreign governments. The comments expressed concern that the CII Act of 2002 did not authorize the Department to share Protected CII with such entities; that express agreements to share Protected CII with foreign governments may be beyond the scope of the Act; and, if sharing information with foreign governments is not beyond the scope of the Act, then senior Department officials, as appropriate, should coordinate the agreements. Comments also questioned how the Department would verify that foreign governments are handling Protected CII appropriately and enforce criminal and administrative penalties if the material is not being handled in a manner consistent with the CII Act of 2002 and this rule. The Department believes that through the establishment of formal agreements with foreign governments, Protected CII can safely and properly be shared for important homeland security purposes. The comments also expressed concern that the proposed rule would allow release of information concerning the source of the Protected CII and other proprietary, business-sensitive information to foreign governments. Accordingly, § 29.8(j) has been revised to address this latter concern by protecting from public disclosure the source of any voluntarily submitted CII that forms the basis for the warning, as well as any information that is proprietary or business sensitive, relates specifically to the submitting party or entity, or is otherwise not appropriate for such disclosure.

Oral Submissions

The Department received one comment expressing concern that oral submission of CII may be chilled by the lack of clarity in the rule concerning the status of notes regarding CII submissions. The comment recommended that the definition of CII be expanded to include notes of oral conversations. The Department intends that notes made by the Protected CII Program Manager or designees shall be presumed to be and will be treated as Protected CII until a validation determination regarding the oral submission and the written version of the oral submission is made otherwise.

The Department received one comment requesting clarification of the process regarding acknowledgement of the receipt of orally submitted CII for protection under the CII Act of 2002. Section 29.6(d) has been revised to explain this process further. In addition, two comments correctly noted that § 29.6(d) was incorrectly numbered in the proposed rule, and the interim rule has been revised accordingly.

Destruction of Information

The Department received three comments noting that the proposed rule used a variety of terms (*e.g.*, "destroy," "dispose," "disposed," and "disposal of") to deal with the treatment of material that has been found not to warrant protection. The comments recommended the consistent use of either "destroy" or "destroyed" throughout the rule in accordance with the Federal Records Act. The interim rule has been revised throughout as appropriate.

Retaining Information for Law Enforcement and/or National Security Reasons

The Department received four comments requesting that the Department clarify what information would be retained for law enforcement and/or national security reasons that would not be Protected CII. The comments requested that language be included to demonstrate that the information would also be protected from disclosure under FOIA. Further, comments recommended that submitters be notified when a submission is retained for such purposes. The Department will retain information for law enforcement and/or national security reasons on a case-by-case basis. In some instances, information that has been found not to warrant protection under the CII Act of 2002 may be of significance for law enforcement and/or national security purposes. In that case, if the information is exempt from disclosure under other FOIA exemptions, the Department will consider such exemptions at the time that a FOIA request is received. In any case, the Department will handle such information in a manner commensurate with its nature and sensitivity.

Deference

The Department received seven comments regarding the deference given to submitters in the Department determination of what is CII. Comments stated that the language is ambiguous and provides too much discretion to the submitter. The Department will evaluate the submitter's claims that information meets the requirements for protection under the CII Act of 2002 and make the final determination regarding whether submitted information meets the requirements for protection. In response to these comments, the Department has removed references to deference. In addition, the Department agreed with two comments suggesting that submitters sign a statement attesting to the validity of their claims that a submission meets the requirements for protection. The Department has added to this interim rule (§ 29.5(a)(4)) the requirement that submitters sign a statement certifying that the submission meets the requirements for protection (*i.e.*, that the information is being provided voluntarily for the purposes of the CII Act of 2002; that the information is not being submitted in lieu of independent compliance with a Federal legal requirement; whether the information is required to be submitted to a Federal agency; and that the information is not customarily in the public domain). It is the intent of this provision to discourage unjustified claims for protection.

Change of Protected CII Status

The Department received 15 comments regarding the change of status from Protected CII to non-Protected CII. The comments recommended that the Protected CII Program Manager notify the submitter and any other parties with whom Protected CII has been shared of any changes in status. The comments also suggested that the circumstances under which a change of status may take place be enumerated in the rule. In response to these comments, § 29.6(f) has been modified to allow the submitter to request in writing that the status of Protected CII material be changed. In addition, the Department recognizes that there may be other circumstances that require the status of Protected CII to be changed. For example, changes may take place if the Program Manager subsequently determines that the information was customarily in the public domain, was required by Federal law or regulation to be submitted to DHS, or is now publicly available through legal means. In addition, § 29.6(f) has been revised to ensure that submitters and those entities with which the Protected CII was shared are made aware of the change in status.

Return and Withdrawal of Material

The Department received seven comments recommending that in addition to maintaining the information without protection and destruction of the information, submitters should be able to indicate that they would like submitted material returned to them in the event that a final validation determination is made that the submission is not Protected CII. Although the Department understands the desire of submitters to retain control over the information that they submitted, including such a provision has the potential to place a significant administrative burden on the Department.

The Department also received one comment requesting that the submitter be provided with the opportunity to withdraw the submission prior to a final validation determination. The Department agrees with this comment and has added language to § 29.6(e)(2)(i)(C) giving submitters an opportunity to withdraw submissions prior to a final validation determination.

Investigation of Violations

The Department received one comment requesting that submitters be notified when an investigation of improper disclosure has begun and the outcome of that investigation, therefore allowing the submitter to take steps to protect information in the event that the material was disclosed improperly. Two additional comments requested that a specific time frame for notification be identified in the rule. The Department disagrees that submitters should be notified when an investigation has begun. It is the Department's belief that at such a time submitters will want to know specific details regarding the suspected or actual violation. The Department will not have specifics until such time as the investigation is concluded and formal findings have been identified.

In addition, one comment was received regarding the requirement that "all persons authorized to have access to Protected CII" report suspected or actual violations. The comment suggested that all officers, employees, contractors, and subcontractors of the Department whether authorized to access Protected CII or not should report suspected or actual violations. The Department does not agree with this suggestion. The intent of § 29.9(a) is to encourage those individuals with access to Protected CII to self-report suspected or actual incidents. In addition, individuals that have not been granted access to Protected CII are unlikely to knowingly witness any abuses of Protected CII procedures. Those authorized to access Protected CII will be uniquely qualified to detect suspected or actual incidents of unauthorized access or misuse.

Whistleblower Protection

The Department received 10 comments suggesting that the application of the Whistleblower Protection Act is not sufficient to protect whistleblowers. The comments expressed concern that whistleblowers could be unfairly treated and subject to termination, fines, and imprisonment. This would discourage the accurate reporting of information vital to the public. The Department has modified

§ 29.8(f)(ii) to reference the Whistleblower Protection Act (WPA). Since the Department's intention is to afford the protections of the WPA, by referencing the WPA itself, the Department believes that it clearly ensures the full range of protections offered under the WPA.

An Appeals Process

The Department received two comments requesting that procedures for appealing determinations regarding Protected CII be included in these regulations. One comment suggested that submitters be provided with additional time to justify their assertion that a submission meets the requirements for protection if the submitter makes such a request. The Department believes that the procedures outlined in § 29.6(e) regarding validation determinations provide submitters with adequate time to justify their submissions. If the Department were to allow appeals of validation determinations or permit submitters to take longer than the thirty calendar days to respond, the Department would be contributing to situations in which information that might not be Protected CII remains in protected status.

No Private Right of Action

The Department received one comment concerning the ambiguity introduced by the proposed rule's reference to "no private rights or privileges" in § 29.3(e). The Department agreed with this comment and has revised the interim rule to ensure that the regulation is consisted with the statutory language. Section 29.3(e) is now entitled "No Private Right of Action."

Restrictions on Use of Protected CII in Civil Actions

The Department received three comments regarding the superfluous and potentially confusing use of the phrase "for homeland security purposes" in § 29.8(i). The Department agrees with these comments and has replaced that phrase with "under the CII Act of 2002."

FOIA Access and Mandatory Submission of Information

The Department received two comments pointing to ambiguities in § 29.3(a) and four comments supporting § 29.3(a). Comments sought to clarify through minor word changes that the provision was intended to prevent submitters from submitting material for protection under the CII Act of 2002 if the material already was required to be submitted to DHS under a Federal legal requirement. The Department agrees in significant part with the intent of the comments to distinguish between submissions of information to different agencies of the Federal government, consistent with the treatment of "independently obtained information" under section 214(c) of the statute, as is discussed in greater detail above. Therefore, § 29.3(a) has been modified accordingly.

Application of Various Laws and Executive Orders to This Interim Rulemaking

Good Cause for Immediate Effectiveness

DHS has determined that it is in the public interest to make this regulation effective upon publication in the **Federal Register**. DHS believes that information that would qualify as Protected CII and would assist DHS in implementing security measures is unlikely to be submitted to DHS before this regulation's effective date. After considering the likelihood that valuable information that likely is now being withheld because of fears that it might be handled without the protections that this regulation would prescribe, and the possibility that this information could be useful in deterring or responding to a security incident, DHS has concluded that the public interest is best served by making the regulation effective immediately.

Regulatory Evaluation

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866, Regulatory Planning and Review (58 FR 51735, October 4, 1993), directs each Federal agency to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (5 U.S.C. 601–612) requires agencies to analyze the economic impact of regulatory changes on small entities. Third, the Office of Management and Budget directs agencies to assess the effect of regulatory changes on international trade. Fourth, the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State or local governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation.)

Executive Order 12866 Assessment

Executive Order 12866 (58 FR 51735, October 4, 1993), provides for making determinations whether a regulatory action is "significant" and therefore subject to Office of Management and Budget (OMB) review and to the requirements of the Executive Order.

DHS has determined that this action is a significant regulatory action within the meaning of Executive Order 12866 because there is significant public interest in security issues since the events of September 11, 2001.

DHS has performed an analysis of the expected costs of this interim rule. The interim rule affects entities in the private sector that have critical infrastructure information that they wish to share with DHS. The interim rule requires that, when DHS receives, validates, and shares CII, DHS and the receiving parties, whether they be other Federal agencies or State or local governments with whom DHS has signed agreements detailing the procedures on how Protected CII must be safeguarded, must take appropriate action to safeguard its contents and to destroy it when it is no longer needed. The interim rule does not require the use of safes or enhanced security equipment or the use of a crosscut shredder. Rather, the interim rule requires only that an affected entity or person restrict disclosure of, and access to, the protected information to those with a need to know, and destroy such information when it is no longer needed. Under the rule, a locked drawer or cabinet is an acceptable means of complying with the requirement to secure Protected CII, and a normal paper shredder or manual destruction are acceptable means of destroying Protected CII documents.

Costs

DHS believes that affected entities will incur minimal costs from complying with the interim rule because, in practice, affected entities already have systems in place for securing sensitive commercial, trade secret, or personnel information, which are appropriate for safeguarding Protected CII. For instance, a normal filing cabinet with a lock may be used to safeguard Protected CII, and a normal paper shredder or manual destruction may be used to destroy CII. Accordingly, the agency estimates that there will be minimal costs associated with safeguarding Protected CII.

The agency has estimated the following costs for placing the required protective marking and distribution

limitation statement on records containing Protected CII.

For an electronic document, a person can place the required markings on each page with a few keystrokes. The agency estimates that there will be no costs associated with this action.

For a document that is already printed, a person can use a rubber stamp for the required markings. Such stamps can be custom ordered and last several years. For the protective marking, the agency estimates that the cost of a rubber stamp is from $9.90 (for a stamp 4¼ inches wide by ¼ inch high) to $10.25 (for a stamp 5 inches wide by ¼ inch high). A typical ink pad costs approximately $15.60. A two-ounce bottle of ink for the ink pad costs about $3.75.

For other types of record, such as maps, photos, DVDs, CD–ROMs, and diskettes, a person can use a label for the required markings. Labels typically cost from $7.87 (for 840 multipurpose labels) to $22.65 (for 225 diskette inkjet labels) to $34.92 (for 30 DVC/CD–ROM labels). These labels can be pre-printed with the required markings, or the affected person can print the required markings on an as-needed basis.

The interim rule does not require a specific method for destroying Protected CII. Thus, a person may use any method of destruction, so long as it precludes recognition or reconstruction of the Protected CII. DHS believes that most affected entities already have the capability to destroy CII in accordance with the requirements in this interim final rule. Thus, the agency estimates that there will be no costs associated with these destruction requirements.

Accordingly, DHS believes that the costs associated with this interim rule are minimal; however, the Department will accept comments addressing the estimated costs associated with the implementation of this rule.

Benefits

The primary benefit of the interim rule will be DHS's ability to receive information from those with direct knowledge on the security of the United States' critical infrastructure, in order to reduce its vulnerability to acts of terrorism by ensuring that information pertaining to the security of critical infrastructure is properly safeguarded and protected from public disclosure. In addition, based on information shared, DHS will provide threat information, security directives, and information circulars throughout the Federal, State, and local governments, to law enforcement officials, to the private sector, and other persons that have a need to know, and to act upon, information about security concerns related to the nation's critical infrastructure.

Prior to providing Protected CII to entities, and to ensure that any information these entities produce that would be treated as Protected CII is safeguarded, DHS must ensure that those entities are under a legal obligation to protect Protected CII from disclosure.

DHS notes that the unauthorized disclosure of Protected CII can have a detrimental effect not only on the ability to thwart terrorist and other criminal activities in the transportation sector, but also on the willingness of the private sector to share that information with DHS if that information might be publicly disclosed.

The effectiveness of providing Protected CII to persons involved with the protection of this country's critical infrastructures, and of security measures developed by those persons, depends on strictly limiting access to the information to those persons who have a need to know. Given the minimal cost associated with this interim rule and the potential benefits of preventing, or mitigating the effects of, terrorist attacks on the United States' critical infrastructures, DHS believes that this interim final will be cost-beneficial; however, the Department will accept comments addressing the anticipated benefits associated with the implementation of this rule.

Initial Regulatory Flexibility Determination

The Regulatory Flexibility Act of 1980, as amended (RFA), was enacted to ensure that small entities are not unnecessarily or disproportionately burdened by Federal regulations. The RFA requires agencies to review rules to determine if they have a "significant impact on a substantial number of small entities." DHS has reviewed this rule and has determined that it will not have a significant economic impact on a substantial number of small entities for the following reasons:

(1) In practice, affected entities already have systems in place for securing sensitive commercial, trade secret, or personnel information, which are appropriate for safeguarding Protected CII. For instance, a normal filing cabinet with a lock may be used to safeguard Protected CII, and a normal paper shredder or manual destruction may be used to destroy CII. Accordingly, the agency estimates that there will be minimal costs associated with safeguarding Protected CII.

(2) The agency has estimated the following costs for placing the required protective marking and distribution limitation statement on records containing Protected CII.

(a) For an electronic document, a person can place the required markings on each page with a few keystrokes. The agency estimates that there will be no costs associated with this action.

(b) For a document that is already printed, a person can use a rubber stamp for the required markings. Such stamps can be custom ordered and last several years. For the protective marking, the agency estimates that the cost of a rubber stamp is from $9.90 (for a stamp 4¼ inches wide by ¼ inch high) to $10.25 (for a stamp 5 inches wide by ¼ inch high). A typical ink pad costs approximately $15.60. A two-ounce bottle of ink for the ink pad costs about $3.75.

(c) For other types of record, such as maps, photos, DVDs, CD–ROMs, and diskettes, a person can use a label for the required markings. Labels typically cost from $7.87 (for 840 multipurpose labels) to $22.65 (for 225 diskette inkjet labels) to $34.92 (for 30 DVC/CD–ROM labels). These labels can be pre-printed with the required markings, or the affected person can print the required markings on an as-needed basis.

(3) The interim rule does not require a specific method for destroying Protected CII. Thus, a person may use any method of destruction, so long as it precludes recognition or reconstruction of the Protected CII. DHS believes that most affected entities already have the capability to destroy CII in accordance with the requirements in this interim rule. Thus, the agency estimates that there will be no costs associated with these destruction requirements; however, the Department will accept comments addressing the impact on small entities associated with the implementation of this rule.

Unfunded Mandates Reform Act of 1995

This interim rule will not result in the expenditure by State and local governments, in the aggregate, or by the private sector, of $100 million or more in any one year, and it will not significantly or uniquely affect small governments.

Executive Order 13132—Federalism

The Department of Homeland Security does not believe this interim rule will have substantial direct effects on the States, on the relationship between the national government and the States, or on distribution of power and responsibilities among the various levels of government. States will benefit, however, from this interim rule to the extent that Protected CII is shared with

them. The Department requests comment on the federalism impact of this interim rule.

Paperwork Reduction Act of 1995

Under the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501–3520), a Federal agency must obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations. This rule does not contain provisions for collection of information, does not meet the definition of "information collection" as defined under 5 CFR part 1320, and is therefore exempt from the requirements of the PRA. Accordingly, there is no requirement to obtain OMB approval for information collection.

Environmental Analysis

DHS has analyzed this regulation for purposes of the National Environmental Policy Act and has concluded that this rule will not have any significant impact on the quality of the human environment.

List of Subjects in 6 CFR Part 29

Confidential business information, Reporting and recordkeeping requirements.

Authority and Issuance

■ For the reasons discussed in the preamble, 6 CFR chapter I is amended by adding part 29 to read as follows:

PART 29—PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Sec.
29.1 Purpose and scope.
29.2 Definitions.
29.3 Effect of provisions.
29.4 Protected Critical Infrastructure Information Program administration.
29.5 Requirements for protection.
29.6 Acknowledgment of receipt, validation, and marking.
29.7 Safeguarding of Protected Critical Infrastructure Information.
29.8 Disclosure of Protected Critical Infrastructure Information.
29.9 Investigation and reporting of violation of Protected CII procedures.

Authority: Pub. L. 107–296, 116 Stat. 2135 (6 U.S.C. 1 *et seq.*); 5 U.S.C. 301.

§ 29.1 Purpose and scope.

(a) *Purpose of the rule.* This part implements section 214 of Title II, Subtitle B, of the Homeland Security Act of 2002 through the establishment of uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal government through the Department of Homeland Security. Title II, Subtitle B, of the Homeland Security Act is referred to herein as the Critical Infrastructure Information Act of 2002 (CII Act of 2002). Consistent with the statutory mission of the Department of Homeland Security (DHS) to prevent terrorist attacks within the United States and reduce the vulnerability of the United States to terrorism, it is the policy of DHS to encourage the voluntary submission of CII by safeguarding and protecting that information from unauthorized disclosure and by ensuring that such information is expeditiously and securely shared with appropriate authorities including Federal national security, homeland security, and law enforcement entities and, consistent with the CII Act of 2002, with State and local officials, where doing so may reasonably be expected to assist in preventing, preempting, and disrupting terrorist threats to our homeland. As required by the CII Act of 2002, the procedures established herein include mechanisms regarding:

(1) The acknowledgement of receipt by DHS of voluntarily submitted CII;

(2) The maintenance of the identification of CII voluntarily submitted to DHS for purposes of, and subject to the provisions of the CII Act of 2002;

(3) The receipt, handling, storage, and proper marking of information as Protected CII;

(4) The safeguarding and maintenance of the confidentiality of such information that permits the sharing of such information within the Federal government and with foreign, State, and local governments and government authorities, and the private sector or the general public, in the form of advisories or warnings; and

(5) The issuance of notices and warnings related to the protection of critical infrastructure and protected systems in such a manner as to protect from unauthorized disclosure the identity of the submitting person or entity as well as information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily available in the public domain.

(b) *Scope.* These procedures apply to all Federal agencies that handle, use, or store Protected CII pursuant to the CII Act of 2002. In addition, these procedures apply to United States Government contractors, to foreign, State, and local governments, and to government authorities, pursuant to any necessary express written agreements, treaties, bilateral agreements, or other statutory authority.

§ 29.2 Definitions.

For purposes of this part:

Critical Infrastructure has the definition referenced in section 2 of the Homeland Security Act of 2002 and means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Critical Infrastructure Information, or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII consists of records and information concerning:

(1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms the interstate commerce of the United States, or threatens public health or safety;

(2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk-management planning, or risk audit; or

(3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

Critical Infrastructure Information Program, or CII Program means the maintenance, management, and review of these procedures and of the information provided to DHS in furtherance of the protections provided by the CII Act of 2002.

Information Sharing and Analysis Organization, or ISAO means any formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of:

(1) Gathering and analyzing CII in order to better understand security problems and interdependencies related to critical infrastructure and protected systems in order to ensure the

availability, integrity, and reliability thereof;

(2) Communicating or sharing CII to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to critical infrastructure or protected systems; and

(3) Voluntarily disseminating CII to its members, Federal, State, and local governments, or to any other entities that may be of assistance in carrying out the purposes specified in this section.

Local Government has the same meaning as is established in section 2 of the Homeland Security Act of 2002 and means:

(1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(3) A rural community, unincorporated town or village, or other public entity.

Protected Critical Infrastructure Information, or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in § 29.5. This information maintains its protected status unless DHS's Protected CII Program Manager or the Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

Protected System means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

Purpose of CII has the meaning set forth in section 214(a)(1) of the CII Act of 2002 and includes the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose.

Submission to DHS as referenced in these procedures means any transmittal of CII to the DHS Protected CII Program Manager or the Protected CII Program Manager's designees, as set forth in § 29.5.

Voluntary or Voluntarily, when used in reference to any submission of CII to DHS, means submitted in the absence of DHS's exercise of legal authority to compel access to or submission of such information; such submission may be accomplished by (*i.e.*, come from) a single entity or by an ISAO acting on behalf of its members. In the case of any action brought under the securities laws—as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))—the term "voluntary" does not include information or statements contained in any documents or materials filed, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(i)), with the Securities and Exchange Commission or with Federal banking regulators; and with respect to the submission of CII, it does not include any disclosure or writing that when made accompanies the solicitation of an offer or a sale of securities. The term also explicitly excludes information or statements submitted during a regulatory proceeding or relied upon as a basis for making licensing or permitting determinations.

§ 29.3 Effect of provisions.

(a) *Mandatory submissions of information.* The CII Act of 2002 and these procedures do not apply to or affect any requirement pertaining to information that must be submitted to DHS pursuant to a Federal legal requirement, nor do they pertain to any obligation of any Federal agency to disclose mandatorily submitted information (even where it is identical to information voluntarily submitted to DHS pursuant to the CII Act of 2002). The fact that a person or entity has voluntarily submitted information pursuant to the CII Act of 2002 does not constitute compliance with any requirement to submit that information to a Federal agency under any other provision of law. Information submitted to any other Federal agency pursuant to a Federal legal requirement is not to be marked as submitted or protected under the CII Act of 2002 or otherwise afforded the protection of the CII Act of 2002, provided, however, that such information, if it is separately submitted to DHS pursuant to these procedures, may upon submission to DHS be marked as Protected CII or otherwise afforded the protections of the CII Act of 2002.

(b) *Freedom of Information Act disclosure exemptions.* Information that is separately exempt from disclosure under the Freedom of Information Act or applicable State or local law does not lose its separate exemption protection due to the applicability of these procedures or any failure to follow them.

(c) *Restriction on use of Protected CII by regulatory and other Federal agencies.* No Federal agency shall request, obtain, maintain, or use information protected under the CII Act of 2002 as a substitute for the exercise of its own legal authority to compel access to or submission of that same information. Federal agencies shall not utilize Protected CII for regulatory purposes without the written consent of the submitter or another party on the submitter's behalf.

(d) *Independently obtained information.* These procedures shall not be construed to limit or in any way affect the ability of a Federal, State, or local government entity, agency, or authority, or any third party, under applicable law, to otherwise obtain CII by means of a different law, regulation, rule, or other authority, including such information as is lawfully and customarily disclosed to the public. Independently obtained information does not include any information derived directly or indirectly from Protected CII subsequent to its submission. Nothing in these procedures shall be construed to limit or in any way affect the ability of such entities, agencies, authorities, or third parties to use such information in any manner permitted by law.

(e) *No private right of action.* Nothing contained in these procedures is intended to confer any substantive or procedural right or privilege on any person or entity. Nothing in these procedures shall be construed to create a private right of action for enforcement of any provision of these procedures or a defense to noncompliance with any independently applicable legal obligation.

§ 29.4 Protected Critical Infrastructure Information Program administration.

(a) *IAIP Directorate Program Management.* The Secretary of the Department of Homeland Security hereby designates the Under Secretary of the Information Analysis and Infrastructure Protection (IAIP)

Directorate as the senior DHS official responsible for the direction and administration of the Protected CII Program.

(b) *Appointment of a Protected CII Program Manager.* The Under Secretary for IAIP shall:

(1) Appoint a Protected CII Program Manager within the IAIP Directorate who is responsible to the Under Secretary for the administration of the Protected CII Program;

(2) Commit resources necessary to the effective implementation of the Protected CII Program;

(3) Ensure that sufficient personnel, including such detailees or assignees from other Federal national security, homeland security, or law enforcement entities as the Under Secretary deems appropriate, are assigned to the Protected CII Program to facilitate the expeditious and secure sharing with appropriate authorities, including Federal national security, homeland security, and law enforcement entities and, consistent with the CII Act of 2002, with State and local officials, where doing so may reasonably be expected to assist in preventing, preempting, or disrupting terrorist threats to our homeland; and

(4) Promulgate implementing directives and prepare training materials as appropriate for the proper treatment of Protected CII.

(c) *Appointment of Protected CII Officers.* The Protected CII Program Manager shall establish procedures to ensure that any DHS component or other Federal, State, or local entity that works with Protected CII appoints one or more employees to serve as a Protected CII Officer for the activity in order to carry out the responsibilities stated in paragraph (d) of this section. Persons appointed to these positions shall be fully familiar with these procedures.

(d) *Responsibilities of Protected CII Officers.* Protected CII Officers shall:

(1) Oversee the handling, use, and storage of Protected CII;

(2) Ensure the expeditious and secure sharing of Protected CII with appropriate authorities, as set forth in § 29.1(a) and paragraph (b)(3) of this section;

(3) Establish and maintain an ongoing self-inspection program, to include periodic review and assessment of the entity's handling, use, and storage of Protected CII;

(4) Establish additional procedures as necessary to prevent unauthorized access to Protected CII; and

(5) Ensure prompt and appropriate coordination with the Protected CII Program Manager regarding any request, challenge, or complaint arising out of the implementation of these procedures.

(e) *Protected Critical Infrastructure Information Management System (PCIIMS).* The Protected CII Program Manager or the Protected CII Program Manager's designees shall develop and use an electronic database, to be known as the "Protected Critical Infrastructure Information Management System" (PCIIMS), to record the receipt, acknowledgement, validation, storage, dissemination, and destruction of Protected CII. This compilation of Protected CII shall be safeguarded and protected in accordance with the provisions of the CII Act of 2002.

§ 29.5 Requirements for protection.

(a) CII shall receive the protections of section 214 of the CII Act of 2002 only when:

(1) Such information is voluntarily submitted to the Protected CII Program Manager or the Protected CII Program Manager's designees;

(2) The information is submitted for use by DHS for the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purposes including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland, as evidenced below;

(3) The information is accompanied by an express statement as follows:

(i) In the case of written information or records, through a written marking on the information or records substantially similar to the following: "This information is voluntarily submitted to the Federal government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002"; or

(ii) In the case of oral information, within fifteen calendar days of the oral submission, through a written statement comparable to the one specified above, and a certification as specified below, accompanied by a written or otherwise tangible version of the oral information initially provided; and

(4) The submitted information additionally is accompanied by a statement, signed by the submitting entity, certifying essentially to the following on behalf of the named entity:

(i) The submitter is voluntarily providing the information for the purposes of the CII Act of 2002;

(ii) The information being submitted is not being submitted in lieu of independent compliance with a Federal legal requirement;

(iii) The information is or is not required to be submitted to a Federal agency. If the information is required to be submitted to a Federal agency, the submitter shall identify the Federal agency requiring submission and the legal authority that mandates the submission; and

(iv) The information is of a type not customarily in the public domain.

(b) Information that is not submitted to the Protected CII Program Manager or the Protected CII Program Manager's designees will not qualify for protection under the CII Act of 2002. Any DHS component other than the IAIP Directorate that receives information with a request for protection under the CII Act of 2002, shall immediately forward the information to the Protected CII Program Manager. Only the Protected CII Program Manager or the Protected CII Program Manager's designees are authorized to acknowledge receipt and validate Protected CII pursuant to § 29.6(a).

(c) Federal agencies and DHS components other than the IAIP Directorate shall maintain information as protected by the provisions of the CII Act of 2002 when that information is provided to the agency or component by the Protected CII Program Manager or the Protected CII Program Manager's designees and is marked as required in § 29.6(c).

(d) All submissions seeking Protected CII status shall be regarded as submitted with the presumption of good faith on the part of the submitter.

(e) Submissions must affirm the understanding of the submitter that any false representations on such submissions may constitute a violation of 18 U.S.C. 1001 and are punishable by fine and imprisonment.

§ 29.6 Acknowledgment of receipt, validation, and marking.

(a) *Authorized officials.* Only the Protected CII Program Manager or the Protected CII Program Manager's designees are authorized to acknowledge receipt of and validate information as Protected CII.

(b) *Presumption of protection.* All information submitted in accordance with the procedures set forth herein will be presumed to be and will be treated as Protected CII from the time the information is received by DHS, either through the DHS component or the Protected CII Program Manager or the Protected CII Program Manager's designees. The information shall remain protected unless and until the Protected CII Program Manager or the Protected CII Program Manager's designees render

a final decision that the information is not Protected CII.

(c) *Marking of information.* In addition to markings made pursuant to § 29.5(a) by submitters of CII requesting review, all Protected CII shall be clearly identified through markings made by the Protected CII Program Manager or the Protected CII Program Manager's designees. The Protected CII Program Manager or the Protected CII Program Manager's designees shall mark Protected CII materials as follows: "This document contains Protected CII. In accordance with the provisions of 6 CFR part 29, it is exempt from release under the Freedom of Information Act (5 U.S.C. 552(b)(3)). Unauthorized release may result in civil penalty or other action. It is to be safeguarded and disseminated in accordance with Protected CII Program requirements."

(d) *Acknowledgement of receipt of information.* The Protected CII Program Manager or the Protected CII Program Manager's designees shall acknowledge receipt of information submitted as CII and accompanied by an express statement and certification, and in so doing shall:

(1) Contact the submitter, within thirty calendar days of receipt, by the means of delivery prescribed in procedures developed by the Protected CII Program Manager or the Protected CII Program Manager. In the case of oral submissions, receipt will be acknowledged in writing within thirty calendar days after receipt by the Protected CII Program Manager or the Protected CII Program Manager's designees of a written statement, certification, and documentation of the oral submission, as referenced in § 29.5(a)(3)(ii);

(2) Maintain a database including date of receipt, name of submitter, description of information, manner of acknowledgment, tracking number, and validation status; and

(3) Provide the submitter with a unique tracking number that will accompany the information from the time it is received by the Protected CII Program Manager or the Protected CII Program Manager's designees.

(e) *Validation of information.*

(1) The Protected CII Program Manager or the Protected CII Program Manager's designees shall be responsible for reviewing all submissions that request protection under the CII Act of 2002. The Protected CII Program Manager or the Protected CII Program Manager's designee shall review the submitted information as soon as practicable. If a determination is made that the submitted information meets the requirements for protection, the Protected CII Program Manager or the Protected CII Program Manager's designee shall mark the information as required in paragraph (c) of this section, and disclose it only pursuant to § 29.8.

(2) If the Protected CII Program Manager or the Protected CII Program Manager's designees make an initial determination that the information submitted does not meet the requirements for protection under the CII Act of 2002, the Protected CII Program Manager or the Protected CII Program Manager's designees shall:

(i) Notify the submitter of the initial determination that the information is not considered to be Protected CII. This notification also shall:

(A) Request that the submitter further explain the nature of the information and the submitter's basis for believing the information qualifies for protection under the CII Act of 2002;

(B) Advise the submitter that the Protected CII Program Manager or the Protected CII Program Manager's designees will review any further information provided before rendering a final determination;

(C) Provide the submitter with an opportunity to withdraw the submission;

(D) Notify the submitter that any response to the notification must be received by the Protected CII Program Manager or the Protected CII Program Manager's designees no later than thirty calendar days after the date of the notification; and

(E) Request the submitter to state whether, in the event the Protected CII Program Manager or the Protected CII Program Manager's designees make a final determination that any such information is not Protected CII, the submitter prefers that the information be maintained without the protections of the CII Act of 2002 or be disposed of in accordance with the Federal Records Act.

(ii) If the Protected CII Program Manager or the Protected CII Program Manager's designees, after following the procedures set forth in paragraph (e)(2)(i) of this section, make a final determination that the information is not Protected CII, the Protected CII Program Manager or the Protected CII Program Manager's designees, in accordance with the submitter's written preference, shall maintain the information without protection or following coordination, as appropriate, with other Federal national security, homeland security, or law enforcement authorities, destroy it in accordance with the Federal Records Act unless the Protected CII Program Manager or the Protected CII Program Manager's designees, consistent with the coordination required in this subpart, determine there is a need to retain it for law enforcement and/or national security reasons. The Protected CII Program Manager or the Protected CII Program Manager's designees shall destroy the information within thirty calendar days of making a final determination. If the submitter, however, cannot be notified or the submitter's response is not received within thirty calendar days after the submitter received the notification, as provided in paragraph (e)(2)(i) of this section, the Protected CII Program Manager or the Protected CII Program Manager's designee will destroy the information in accordance with the Federal Records Act, unless the Protected CII Program Manager or the Protected CII Program Manager's designee, after coordination with other Federal national security, homeland security, or law enforcement authorities, as appropriate, determines that there is a need to retain it for law enforcement and/or national security reasons.

(f) *Changing the status of Protected CII to non-Protected CII.* Once information is validated, only the Protected CII Program Manager or the Protected CII Program Manager's designees may change the status of Protected CII to that of non-Protected CII and remove its Protected CII markings. Status changes may take place when the submitter requests in writing that the information no longer be protected under the CII Act of 2002 or when the Protected CII Program Manager or the Protected CII Program Manager's designee determines that the information was customarily in the public domain, is publicly available through legal means, or is required to be submitted to DHS by Federal law or regulation. The Protected CII Program Manager or the Protected CII Program Manager's designees shall inform the submitter when a change in status is made. Notice of the change in status of Protected CII shall be provided to all recipients of that Protected CII under § 29.8.

§ 29.7 Safeguarding of Protected Critical Infrastructure Information.

(a) *Safeguarding.* All persons granted access to Protected CII are responsible for safeguarding all such information in their possession or control. Protected CII shall be protected at all times by appropriate storage and handling. Each person who works with Protected CII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

(b) *Use and storage.* When Protected CII is in the physical possession of a person, reasonable steps shall be taken to minimize the risk of access to Protected CII by unauthorized persons. When Protected CII is not in the physical possession of a person, it shall be stored in a secure environment that affords it the necessary level of protection commensurate with its vulnerability and sensitivity.

(c) *Reproduction.* Pursuant to procedures prescribed by the Protected CII Program Manager, a document or other material containing PCII may be reproduced to the extent necessary consistent with the need to carry out official duties, provided that the reproduced documents or material are marked and protected in the same manner as the original documents or material.

(d) *Disposal of information.* Documents and material containing Protected CII may be disposed of by any method that prevents unauthorized retrieval.

(e) *Transmission of information.* Protected CII shall be transmitted only by secure means of delivery as determined by the Protected CII Program Manager or the Protected CII Program Manager's designees.

(f) *Automated Information Systems.* The Protected CII Program Manager or the Protected CII Program Manager's designees shall establish security requirements for Automated Information Systems that contain Protected CII.

§ 29.8 Disclosure of Protected Critical Infrastructure Information.

(a) *Authorization of access.* The Under Secretary for IAIP, or the Under Secretary's designee, may choose to provide or authorize access to Protected CII when it is determined that this access supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, other law, regulation, or legal authority. Any disclosure or use of Protected CII within the Federal government is limited by the terms of the CII Act of 2002. Accordingly, any advisories, alerts, or warnings issued to the public pursuant to paragraph (e) of this section shall protect from disclosure:

(1) The source of any voluntarily submitted CII that forms the basis for the warning, and

(2) Any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain.

(b) *Federal, State, and local government sharing.* The Protected CII Program Manager or the Protected CII Program Manager's designees may provide Protected CII to an employee of the Federal government, or of a State or local government, provided that such information is shared for purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland. Protected CII may be provided to a State or local government entity only pursuant to its express written agreement with the Protected CII Program Manager to comply with the requirements of paragraph (d) of this section and that acknowledges the understanding and responsibilities of the recipient.

(c) *Disclosure of information to Federal contractors.* Disclosure of Protected CII to Federal contractors may be made only after the Protected CII Program Manager or a Protected CII Officer certifies that the contractor is performing services in support of the purposes of DHS, the contractor has signed corporate or individual confidentiality agreements as appropriate, covering an identified category of contractor employees where appropriate, and has agreed by contract to comply with all the requirements of the Protected CII Program. The contractor shall safeguard Protected CII in accordance with these procedures and shall not remove any "Protected CII" markings. Contractors shall not further disclose Protected CII to any of their components, additional employees, or other contractors (including subcontractors) without the prior written approval of the Protected CII Program Manager or the Protected CII Program Manager's designees, unless such disclosure is expressly authorized in writing by the submitter and is the subject of timely notification to the Protected CII Program Manager.

(d) *Further use or disclosure of information by State and local governments.*

(1) State and local governments receiving information marked "Protected Critical Infrastructure Information" shall not share that information with any other party, or remove any Protected CII markings, without first obtaining authorization from the Protected CII Program Manager or the Protected CII Program Manager's designees who shall be responsible for requesting and obtaining written consent for any such State or local government disclosure from the person or entity that submitted the information or on whose behalf the information was submitted.

(2) The Protected CII Program Manager or a Protected CII Program Manager's designee may not authorize State and local governments to further disclose the information to another party unless the Protected CII Program Manager or a Protected CII Program Manager's designee first obtains the written consent of the person or entity submitting the information.

(3) State and local governments may use Protected CII only for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act

(e) *Disclosure of information to appropriate entities or to the general public.* The IAIP Directorate may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, ISAOs or the general public regarding potential threats and vulnerabilities to critical infrastructure as appropriate. In issuing a warning, the IAIP Directorate shall protect from disclosure the source of any Protected CII that forms the basis for the warning as well as any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain.

(f) *Access by Congress and whistleblower protection.*

(1) Exceptions for disclosure.

(i) Pursuant to section 214(a)(1)(D) of the CII Act of 2002, Protected CII shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of the CII Act of 2002, except—

(A) In furtherance of an investigation or the prosecution of a criminal act; or

(B) When disclosure of the information is made—

(*1*) To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(*2*) To the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

(ii) If any officer or employee of the United States makes any disclosure pursuant to these exceptions, contemporaneous written notification must be provided to the Department through the Protected CII Program Manager.

(2) Consistent with the authority to disclose information for any purpose described in § 29.2, disclosure of Protected CII may be made, without the written consent of the person or entity submitting such information, to the DHS Inspector General, or to any other employee designated by the Secretary of Homeland Security.

(3) Subject to the limitations of title 5 U.S.C., section 1213 (the "Whistleblower Protection Act"), disclosure of Protected CII may be made by any officer or employee of the United States who reasonably believes that such information:

(i) Evidences an employee's or agency's conduct in violation of criminal law, or any other law, rule, or regulation, affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or reconstitution or

(ii) Evidences mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or reconstitution.

(4) Disclosures of all of the information cited in paragraphs (f)(1) through (3) of this section, including under paragraph (f)(1)(i)(A), are authorized by law and therefore are not subject to penalty under section 214(f) of the Homeland Security Act of 2002.

(g) *Responding to requests made under the Freedom of Information Act or State/local information access laws.*

(1) Protected CII shall be treated as exempt from disclosure under the Freedom of Information Act and, if provided by the Protected CII Program Manager or the Protected CII Program Manager's designees to a State or local government agency, entity, or authority, or an employee or contractor thereof, shall not be made available pursuant to any State or local law requiring disclosure of records or information. Any Federal, State, or local government agency with questions regarding the protection of Protected CII from public disclosure shall contact the Protected CII Program Manager, who shall in turn consult with the DHS Office of the General Counsel.

(2) These procedures do not limit or otherwise affect the ability of a State or local government entity, agency, or authority to obtain under applicable State or local law information directly from the same person or entity voluntarily submitting information to DHS. Information independently obtained by a State or local government entity, agency, or authority is not subject to the CII Act of 2002's prohibition on making such information available pursuant to any State or local law requiring disclosure of records or information.

(h) *Ex parte communications with decisionmaking officials.* Pursuant to section 214(a)(1)(B) of the Homeland Security Act of 2002, Protected CII is not subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official.

(i) *Restriction on use of Protected CII in civil actions.* Pursuant to section 214(a)(1)(C) of the Homeland Security Act of 2002, Protected CII shall not, without the written consent of the person or entity submitting such information, be used directly by any Federal, State, or local authority, or by any third party, in any civil action arising under Federal or State law if such information is submitted in good faith under the CII Act of 2002.

(j) *Disclosure to foreign governments.* The Protected CII Program Manager or the Protected CII Program Manager's designees may provide Protected CII to a foreign Government without the written consent of the person or entity submitting such information to the same extent, and under the same conditions, it may provide advisories, alerts, and warnings to other governmental entities as described in paragraph (e) of this section, or in furtherance of an investigation or the prosecution of a criminal act. Before disclosing Protected CII to a foreign government, the Protected CII Program Manager or the Protected CII Program Manager's designees shall protect from disclosure the source of the Protected CII, any information that is proprietary or business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriate for such disclosure.

(k) *Obtaining written consent for further disclosure from the person or entity submitting information.*

(1) Authority to Seek and Obtain Submitter's Consent to Disclosure. The Protected CII Program Manager or any Protected CII Program Manager's designee may seek and obtain written consent from persons or entities submitting information when such consent is required under the CII Act of 2002 to permit disclosure. In exigent circumstances, and so long as contemporaneous notice is provided to the Protected CII Program Manager or the Protected CII Program Manager's designees, any Federal government employee may seek the consent of the submitting party to the disclosure of Protected CII where such consent is required under the CII Act of 2002.

(2) Consequence of Consent. Whether given in response to a request from the Protected CII Program Manager, the Protected CII Program Manager's designees, or another Federal government employee pursuant to paragraph (k)(1) of this section, a person's or entity's consent to additional disclosure, if conditioned on a limited release of Protected CII that is made for DHS's purposes and in a manner that offers reasonable protection against disclosure to the general public, shall not result in the information's loss of treatment as Protected CII.

§ 29.9 Investigation and reporting of violation of protected CII procedures.

(a) *Reporting of possible violations.* Persons authorized to have access to Protected CII shall report any possible violation of security procedures, the loss or misplacement of Protected CII, and any unauthorized disclosure of Protected CII immediately to the Protected CII Program Manager or the Protected CII Program Manager's designees who shall in turn report the incident to the IAIP Directorate Security Officer and to the DHS Inspector General.

(b) *Review and investigation of written report.* The Inspector General, Protected CII Program Manager, or IAIP Security Officer shall investigate the incident and, in consultation with the DHS Office of the General Counsel, determine whether a violation of procedures, loss of information, and/or unauthorized disclosure has occurred. If the investigation reveals any evidence of wrongdoing, DHS, through its Office of the General Counsel, shall immediately contact the Department of Justice's Criminal Division for consideration of prosecution under the criminal penalty provisions of section 214(f) of the CII Act of 2002.

(c) *Notification to originator of Protected CII.* If the Protected CII Program Manager or the IAIP Security Officer determines that a loss of information or an unauthorized disclosure has occurred, the Protected CII Program Manager or the Protected CII Program Manager's designees shall notify the submitter of the information in writing, unless providing such notification could reasonably be expected to harm the investigation of that loss or any other law enforcement, national security, or homeland security interest. The written notice shall contain a description of the incident and the date of disclosure, if known.

(d) *Criminal and administrative penalties.* As established in section 214(f) of the CII Act, whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information protected from disclosure by the CII Act of 2002 and coming to the officer or employee in the course of his or her employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than one year, or both, and shall be removed from office or employment.

Dated: February 12, 2004.

Tom Ridge,

Secretary of Homeland Security.

[FR Doc. 04–3641 Filed 2–19–04; 8:45 am]

BILLING CODE 4410–10–P

April 13, 2004

The Honorable Susan M. Collins
United States Senate
Washington, D.C. 20510

The Honorable Carl Levin
United States Senate
Washington, D.C. 20510

Dear Senator Collins and Senator Levin:

Thank you for your letter regarding the division of responsibility among certain counterterrorism elements of the United States Government (USG). We have provided you and your staff with information describing the mission, responsibilities, and relationships of the Terrorist Threat Integration Center (TTIC), the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate (IAIP), and other government elements with terrorism analysis responsibilities. Based on your questions, this letter focuses on counterterrorism analysis within the Federal government.

Primary Responsibility for Terrorism Information Analysis

TTIC has the primary responsibility in the USG for terrorism analysis (except information relating solely to purely domestic terrorism) and is responsible for the day-to-day terrorism analysis provided to the President and other senior policymakers. We presume that all terrorism information has a link to international terrorism unless determined otherwise. Where information has been determined to have no such link to international terrorism, the FBI has primary responsibility with regard to the analysis of such information. This FBI responsibility, like TTIC's, is independent of where the information was collected.

IAIP has the primary responsibility for matching the assessment of the risk posed by identified threats and terrorist capabilities to our Nation's vulnerabilities. IAIP is also responsible for providing the full-range of intelligence support -- briefings, analytic products, including competitive analysis, "red teaming," and tailored analysis responding to specific inquiries -- to the DHS Secretary, other DHS leadership, and the rest of DHS. DHS also has significant responsibilities with regard to "purely domestic" terrorism threats, particularly in support of its critical infrastructure protection, Customs, immigration, and other statutory responsibilities.

USG counterterrorism elements retain such terrorism analytic responsibility and capability as necessary to support their own counterterrorism mission, and to carry out specific functions assigned to them by statute or Presidential directive.

Terrorist Threat Integration Center (TTIC)

TTIC has no operational authority. However, TTIC has the authority to task collection and analysis from Intelligence Community agencies, the FBI, and DHS through tasking mechanisms we will create. The analytic work conducted at TTIC creates products that inform each of TTIC's partner elements, as well as other Federal departments and agencies as appropriate. These products are produced collaboratively by all of these elements, principally through their assignees physically located at the TTIC facility, but also working closely with their headquarters elements.

The DCI Counterterrorism Center (CTC)

The Director of Central Intelligence Counterterrorism Center (CTC) conducts worldwide operations and collection activities to detect, disrupt, and preempt actions of al-Qa'ida and other terrorist groups. CTC continues to conduct analysis to support its mission. CTC may conduct other analysis at the direction of the DCI or at the request of the Director of TTIC. The DCI, in consultation with the other leaders of the Intelligence Community and no later than June 1, 2004, will determine what additional analytic resources will be transferred to TTIC.

DHS Directorate of Information Analysis and Infrastructure Protection (IAIP)

Whereas TTIC's terrorism analytic mission is global in nature, IAIP's mission is singularly focused on the protection of the American homeland against terrorist attack. This is unique among all intelligence, law enforcement, and military entities whose missions both extend worldwide and to subject-matter areas and purposes well beyond counterterrorism. This focus allows IAIP to concentrate its energy on protecting against threats to homeland targets, while working closely with other USG components that have overseas-focused, or both overseas- and domestic-focused, missions, to ensure unity of purpose and effort against terrorism worldwide. IAIP brings several unique capabilities to the US Government. The Directorate maps terrorist threats to the homeland against our assessed vulnerabilities in order to drive our efforts to protect against terrorist attacks. Furthermore, through its combination of intelligence analysis and infrastructure assessment, IAIP is able to independently analyze information from multiple Intelligence Community sources, as well as from its fellow DHS entities. Lastly, IAIP is able to provide key information to the American citizenry, accompanied by suggested protective measures.

IAIP's singular focus on the homeland allows it to carry out all missions assigned to it by the Homeland Security Act, including the following:

- Facilitating the creation of requirements, on behalf of the Secretary of Homeland Security and DHS leadership, to other DHS components, and to the larger intelligence, law enforcement, and homeland security communities, in order to integrate homeland security information from all sources with vulnerability and risk assessments for critical infrastructure prepared by IAIP;

- Providing the full-range of intelligence support -- briefings, analytic products, including competitive analysis, "red teaming," and tailored analysis responding to specific inquiries, and other support -- to the DHS leadership and the rest of DHS;

- Working with the FBI and others to ensure that homeland security-related intelligence information is shared with others who need it, in the Federal, state, and local governments, as well as in the private sector;

- Serving as the manager for collection, processing, integration, analysis, and dissemination for DHS' information collection and operational components (Coast Guard, Secret Service, Transportation Security Administration, Immigration and Customs Enforcement, Customs and Border Protection), turning the voluminous potentially threat-related information collected every day at our borders, ports, and airports, into usable and, in many cases, actionable intelligence; and

- Supporting the DHS Secretary's responsibility to administer the Homeland Security Advisory System, including independently analyzing information supporting decisions to raise or lower the national warning level.

FBI

The FBI's Counterterrorism Division (CTD) has three core responsibilities: 1) managing counterterrorism operations on the territory of the United States to detect, disrupt, and preempt terrorist activities; 2) conducting analysis to support its own operations; and 3) producing and disseminating to all Federal counterterrorism elements and, as appropriate, State and local law enforcement officials, intelligence reports resulting from these operations.

FBI analysts within CTD exploit all available intelligence and information to drive FBI terrorism operations that will lead to the identification and disruption of terrorist activities. FBI also has the responsibility for analyzing law enforcement and investigative information that has been determined to have no connection to international terrorism.

It is important to identify the role of the new FBI's Office of Intelligence as it relates to the division of responsibility among certain USG counterterrorism elements. The FBI Office of Intelligence, which provides CTD's imbedded analytic capability, also performs the analytic work necessary to inform the FBI's collection tasking. This analytic product is designed purely to guide the work of the FBI in responding to collection requirements. In addition, the Office of Intelligence provides the full range of intelligence support to FBI components.

Finally, working with IAIP, TTIC, and other USG counterterrorism elements, CTD and the FBI Office of Intelligence ensure that all terrorism information collected by FBI, both abroad and within the United States, is shared with, and integrated into the work of, other USG counterterrorism elements in accordance with law, Presidential policy and direction, and written agreements such as those referenced herein.

Conclusion

Regardless of the particular analytic roles of any USG counterterrorism element under our control, we have committed all such elements, consistent with the President's policies, to share terrorism information (as defined by the Memorandum of Understanding on Information Sharing, dated March 4, 2003) with one another to ensure a seamless integration of such

information. Nothing in this explanatory letter is intended to modify the definitions or obligations of this MOU or other relevant directives or agreements.

The President and Congress have not directed, and, as a matter of effective government and common sense, should not direct, that all USG functions related to terrorism, including defense, intelligence, domestic law enforcement, diplomatic, economic, and a host of others be carried out by a single department or agency. In order both to ensure that no vital piece of intelligence is missed and to ensure that all departments and agencies, as well as our national leadership, receive the best possible analytic support, it is necessary to treat the analysis of terrorism-related information as a shared responsibility.

We look forward to continuing to work with your Committee as we strive to enhance our ability to protect our Nation from terrorists seeking to harm us. If you have any questions about this matter, then please have your staff contact Phil Lago with the Director of Central Intelligence at 703-482-6590, or Eleni Kalisch with the Director of the Federal Bureau of Investigation at 202-324-5051, or Ken Hill with the Secretary of Homeland Security at 202-282-8222, or Cynthia Bower with the Director of the Terrorist Threat Integration Center at 703-482-3354.

Sincerely,

Tom Ridge

Thomas J. Ridge
Secretary,
Department of Homeland Security

Robert S. Mueller III
Director,
Federal Bureau of Investigation

George J. Tenet
Director of Central Intelligence

John O. Brennan
Director,
Terrorist Threat Integration Center

Attachment 2 to Ridge 9 Feb 04 QFRs

FACT SHEET:
DHS Directorate of Information Analysis and Infrastructure Protection

Summary

The Directorate of Information Analysis and Infrastructure Protection ("IAIP") of the Department of Homeland Security (DHS) is firmly committed to carrying out each of the 19 responsibilities assigned to it in Section 201 of the Homeland Security Act. As indicated in the Reorganization Plan, submitted to Congress on November 22, 2002, and graphically represented in the attached table, the Office of Information Analysis ("IA") will carry out 16 of the 19 responsibilities (working together with the Office of Infrastructure Protection ("IP") on seven of these). IP itself will carry out three of the 19. IA will carry out one of the 19 responsibilities -- identifying, detecting, and assessing terrorist threats to the homeland -- both through analysts at DHS Headquarters and through operating as one of the Terrorist Threat Integration Center ("TTIC") partners in collaboration with analysts from other key agencies. Although only a few months old, IAIP is moving forward to increase its staff to carry out these statutory responsibilities, and will have 86 full time analysts by September 2003, and 113 by March 2004. Among the key missions of IA, which it is now carrying out and for which IA will continue to increase its capability, are:

- Providing the full range of intelligence support to senior DHS leadership, as do intelligence components of other departments and agencies;

- With IP, mapping terrorist threats to the homeland against our assessed vulnerabilities in order to drive our efforts to protect against terrorist attacks;

- Conducting independent analysis of terrorist threats to the homeland based on DHS' robust access to information and intelligence, including competitive analysis, tailored analysis, and "red teaming;"

- Supporting the work of all of DHS' components, including the Directorates of Border and Transportation Security, Science and Technology, and Emergency Preparedness and Response. This analytic support will also be provided to DHS' decisionmakers under pending Bioshield legislation, if enacted;

- Analyzing terrorist threats to the homeland, both at DHS Headquarters, and through IA analysts physically located at TTIC;

- Developing requirements for the collection of intelligence and other information related to terrorist threats to the homeland for use by the Intelligence Community and U.S. law enforcement agencies;

- Coordinating exchanges of terrorist threat-related information with state and local governments and the private sector; and

- Managing the collection and processing of information into usable intelligence from DHS' inherited intelligence components, e.g., Customs, Coast Guard, Secret Service.

To carry out these critical responsibilities, the President and Congress have provided DHS/IAIP with unique and powerful authorities and capabilities, outlined in greater detail below.

A Unique Organization. IAIP is unique among federal agencies with intelligence and law enforcement functions in terms of its combination of authority, responsibility, and access to information. No other entity combines IAIP's:

- Robust, comprehensive, and independent access, mandated by the President and in the law, to information relevant to homeland security, whether raw or processed;
- Mission and authority to obtain information and intelligence, including through DHS components, analyze that data, and take action to prevent, and respond to, terrorist attacks directed at the U.S. homeland; and
- Ability to conduct its own, independent threat and other analysis and to leverage the analytic resources of the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), Department of Defense (DOD), TTIC, and other entities, to manage the protection of the homeland.

IAIP - Focus on the Homeland. IAIP's anti-terrorism mission is singularly focused on the protection of the American homeland against terrorist attack. This is unique among all intelligence, law enforcement, and military entities (such as CIA, FBI, and DOD), whose missions extend both worldwide, and to subject-matter areas and purposes well beyond anti-terrorism. This focus allows IAIP to concentrate its energy on protecting against threats at home, while working closely with other U.S. Government components with explicit overseas-focused, or both overseas- and domestic-focused, missions to ensure unity of purpose and effort against terrorist threats worldwide. Precisely because DHS/IAIP is domestically focused, it can concentrate its considerable authorities and capabilities on a critical mission that was fragmented prior to the President's proposal to create DHS: protecting against terrorist attacks at home.

Central Role. Central to the success of this singular DHS mission is the coordination of the Office of Information Analysis ("IA) with the Office of Infrastructure Protection ("IP") to ensure that threat information is correlated with critical infrastructure vulnerabilities and protective programs. This correlation provides the essential context to determine the relevance and efficacy of threat information to the protection of critical infrastructure components and key assets. IAIP is the center of strategy coordination for all of DHS' Critical Infrastructure Protection efforts. Working through its Headquarters-based analysts, IA, in close collaboration and coordination with IP, will choreograph an interactive relationship between analysis of terrorist threats against the United States homeland, comprehensive vulnerability assessments, and domestic preventative and protective measures. The IA-IP partnership significantly reduces the potential for intelligence gaps and communications failures. This linkage of information access and analysis on the one hand and vulnerabilities analysis and protective measures on the other is what is entirely new, and unduplicated elsewhere, about the President's vision for DHS.

Partnership with State and Local Governments and the Private Sector. Unlike other members of the Intelligence Community, including others represented at the TTIC, IA has both the authority and responsibility for providing Federally-collected and analyzed homeland security information to first responders and other state and local officials and, as appropriate, security managers and other key private sector contacts. Likewise, only IA, in coordination with IP, is in the position effectively to manage the collection from state and local governments, and private sector officials, of the crucial homeland security-related information that may be, in the first instance, available only to those officials. DHS will work closely with other U.S. Government agencies to coordinate relations with state, local, and private sector officials, including coordinating with FBI on contacts with state and local law enforcement.

Beyond the unique IA-IP partnership, IA is also the central information nerve center of DHS' efforts to coordinate the protection of U.S. homeland security. IA will:

- Facilitate the creation of **requirements**, on behalf of the Secretary and DHS leadership, to other DHS components, and to the Intelligence Community, and law enforcement, informed by the integration of homeland-security-related intelligence from all sources with vulnerability and risk assessments for critical infrastructure prepared by IP;

- Provide the full-range **of intelligence support** -- briefings, analytic products, including tailored analysis responding to specific inquiries, and other support -- to the Secretary, DHS leadership, the Undersecretary for IAIP, and DHS' operational components, as well as the rest of DHS;

- Serve as the **gathering, processing, integration, analytic, and dissemination manager** for DHS Headquarters and operational components (Coast Guard, Secret Service, Transportation Security Administration, Immigration and Customs Enforcement, Customs and Border Protection), turning the voluminous threat information collected every day at our borders, ports, and airports, into usable and, in many cases, actionable intelligence;

- **Ensure** (in coordination with FBI and others) that homeland security-related intelligence **information is shared** with others who need it, in the Federal, state, and local governments, as well as the private sector; and

- **Support the Homeland Security Advisory System.** IA's activities also will be in support of the Secretary's responsibility to administer the Homeland Security Advisory System, including independently analyzing information supporting decisions to raise or lower the national warning level.

Terrorism Threat Analysis: IA and TTIC. In addition to mapping terrorism threats to the homeland, and carrying out its many other intelligence analytic functions, IA, as directed by the President and Congress, will identify, detect, and assess the nature and scope of terrorist threats to the homeland. Some of DHS' work in this area will be carried out in part by IA analysts who are full participants in the President's Terrorism

Threat Integration Center (TTIC) initiative, and physically located at TTIC. Other threat analysis will be carried out by IAIP analysts located at Headquarters, in close coordination with those located at TTIC.

IA "Doing Business As" TTIC

Certain IA officers will be located at TTIC, working day-in-day-out, participating in processing and analyzing terrorist threat-related information, developing, shaping, and disseminating TTIC products, assessing gaps in the available information, and ensuring that TTIC products reach appropriate DHS Headquarters elements, as well as appropriate state, local, and private sector officials. IA analysts assigned to TTIC will ensure that information gathered by DHS (from its own collectors as well as state and local governments and the private sector) reaches TTIC and informs its work and, equally important, that TTIC's work directly supports DHS' unique mission to protect the homeland. IA analysts at TTIC are there, in significant part, to carry out DHS' mission. The threat information integration and analysis that is the beginning, not the end, of DHS' protective mission, will most effectively be carried out, as Congressional and other reviews have recommended, when all terrorism threat-related activities of the U.S. Government work together seamlessly. This includes counter-terrorism activities directed against threats overseas, as well as criminal investigation and prosecution activities, which the President and Congress did not, and, as a matter of effective government and common sense, should not, direct be carried out exclusively by DHS.

Leveraging Co-Located Resources

With the early fall 2004 co-location of TTIC (including the IA analysts working for DHS there), with CIA's Counterterrorist Center, and the FBI's Counterterrorism Division, DHS will be able to leverage the presence of its personnel at this combined facility to: reduce transmission and coordination time for critical information; and facilitate comprehensive assessment of not only domestic threats but also foreign-based threats that may ultimately impact the homeland. As provided by Congress and the President, authorities and capabilities to deter and disrupt terrorist threats, particularly overseas, are shared among a number of departments and agencies and such activities often must be undertaken in concert with state, local, and foreign governments. Recent experience has shown that terrorist groups may attempt to coordinate multiple attacks, both overseas and within the United States, and that threats that appear to be directed overseas may actually be directed towards the homeland, and vice versa.

Robust and Independent Access to Intelligence

To carry out portions of its mission performed by IA analysts physically located at TTIC and those at DHS Headquarters, IA will have robust, comprehensive, and independent access, mandated by the President and in the law, to information relevant to homeland security, whether raw or processed. IA's access is not an "either" IA at TTIC "or" IA at DHS Headquarters issue. IA will have the mandated access to, and the physical electronic means to receive information, independent of its participation in the TTIC. DHS' robust access to homeland security information -- provided by the President, by Congress, and by written agreement between the Secretary, Director of

Central Intelligence, and Attorney General -- is in no way limited to those IA officers physically working at TTIC. A copy of the Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing, dated March 4, 2003 ("the MOU") is attached hereto.

Leveraging Federal, State and Local Information, and DHS/IP

In carrying out their analysis, IA analysts at DHS Headquarters not only will have access to all relevant information from U.S. intelligence and law enforcement agencies and from officials in state and local governments and the private sector, but they will be able to reach out, via the IA analysts located at TTIC, to leverage their expertise and direct contacts to the overall U.S. counterterrorism operational and analytic efforts co-located there. DHS/IP will rely upon the analysis produced by IA, to help determine priorities for protective and support measures and provide them to federal, state, and local government agencies and authorities, and to private sector entities. In support of its mission, DHS/IP will drive, through and with IA, requirements to the Intelligence Community, law enforcement, and other parts of DHS, to ensure that vulnerabilities and threats are correlated and appropriate protective actions are defined and implemented.

IA's Independent Analytic Work

In addition to the critical role, outlined above, of mapping infrastructure vulnerabilities against threats to the homeland, IA also will conduct other analysis distinct from that in which IA analysts participate at TTIC, including:

- **Tailored Analysis**. IA Headquarters-based analysts will routinely be tasked to take a different "cut" at a similar universe of information as that analyzed at TTIC. For example, TTIC may reach a conclusion about a general terrorist threat to the United States, while DHS Headquarters may want a more targeted and specific analysis directed at how such a threat might affect a particular sector of the U.S. infrastructure. Such threat analysis would be different than that performed at TTIC, but crucial to the overall DHS mission and to our homeland security. Similar tailored analytic products are systematically used by the leaders of other Intelligence Community member Departments and Agencies based on each agency's individual mission.

- **Competitive Analysis**. IAIP analysts located at Headquarters will also conduct competitive terrorism threat analysis to that taking place at TTIC. For example, the Secretary may want an independent look at a particular conclusion reached by analysts – including IA analysts – at TTIC. Such competitive analysis not only is sound practice, but it has been for decades a cornerstone of U.S. Intelligence Community analytic efforts.

- **Red-Teaming**. IA's tailored and, at times, competitive terrorism threat analysis, will take another form as well: "red teaming." IA's analysts will not only look independently at threat data from a traditional analytical perspective, i.e., "connecting the dots," but will also undertake "red team" analysis. In this mode, analysts will view the United States from the perspective of the terrorists, seeking to discern and

predict the methods, means and targets of the terrorists. The analysis produced as part of this red teaming will then be utilized to uncover weaknesses, and to set priorities for long-term protective action and target hardening.

TTIC's Mission

TTIC is an interagency joint venture of its partners. The TTIC members include, but are not limited to, the Department of Justice/FBI, DHS, CIA, National Security Agency, National Imagery and Mapping Agency, Defense Intelligence Agency, and the Department of State. Through the input and participation of these partners, TTIC will merge and analyze terrorist threat-related information, collected domestically and abroad, in order to form the most comprehensive possible threat picture, and disseminate such information to appropriate recipients. TTIC, through its structure, will draw on the particular expertise of its participating members – such as DHS' focus on homeland security and CIA's focus on terrorism information collected overseas – thereby ensuring that the terrorist analytic product takes advantage of, and incorporates, the specialized perspectives of relevant federal agencies. In addition, TTIC will have access to, and will aggressively seek to analyze, information from state and local entities, as well as voluntarily provided data from the private sector. TTIC will work with appropriate partners to ensure that TTIC's products reach not only federal customers, but also state and local, as well as private sector, partners.

TTIC will provide comprehensive, all-source terrorist threat analysis and assessments to U.S. national leadership. It will also play a lead role, along with other organizations, in overseeing a national terrorist threat tasking and requirements system. In addition, TTIC will maintain an up-to-date database of known and suspected terrorists accessible to appropriate officials. A copy of Director of Central Intelligence Directive 2/4, concerning TTIC, is attached hereto.

Attachment 2 to Ridge 9 Feb 04 QFRs

Statutory Function*	**Component**	**Performed, in Part, at TTIC?**
Vulnerabilities Assessment	IP	**NO**
National Plan to Secure Infrastructure	IP	**NO**
Recommend Infrastructure Protective Measures	IP	**NO**
"Map" threats against vulnerabilities	IA/IP	**NO**
Ensure timely and efficient access to DHS of all homeland security information	IA	**NO**
Administer the Homeland Security Advisory System	IA	**NO**
Make recommendations for homeland security information sharing policies	IA	**NO**
Disseminate information analyzed by DHS to other federal, state, and local government entities and the private sector	IA	**NO**
Consult with appropriate federal Intelligence Community and law enforcement officials to establish collection priorities and strategies and represent DHS in "requirements" processes	IA	**NO**
Consult with state and local governments and the private sector to ensure appropriate exchanges of terrorist threat-related information	IA	**NO**
Ensure that information received is protected from unauthorized disclosure and handled and used only for the performance of official duties	IA/IP	**NO**
Request additional information from other federal, state, local government agencies and the private sector	IA/IP	**NO**
Establish and use secure information technology infrastructure	IA/IP	**NO**
Ensure that information systems/databases are compatible with one another and other federal agencies and treat information in accordance with applicable Federal privacy law	IA/IP	**NO**
Coordinate training and other support to DHS and other agencies to identify and share information	IA/IP	**NO**
Coordinate with IC elements and federal, state, and local law enforcement agencies "as appropriate"	IA	**NO**
Provide intelligence analysis and other support to the rest of DHS	IA	**NO**
Perform such other duties as the Secretary may provide	IA/IP	**NO**
Identify, Detect, and Assess Terrorist Threats to Homeland	IA	**YES**

* This chart is intended only to describe in general terms IAIP's division of labor with regard to functions assigned DHS by the Homeland Security Act. Other parts of DHS, as well as participants in TTIC and all other federal Departments and Agencies, remain responsible, with regard to their own work and information in their possession, for many of these same functions, e.g., protecting information against unauthorized disclosure.