AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 110–528

NOMINATIONS OF ROBERT D. JAMISON AND W. ROSS ASHLEY III

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

ROBERT D. JAMISON TO BE UNDER SECRETARY FOR NATIONAL PROTECTION AND PROGRAMS, AND W. ROSS ASHLEY III TO BE ASSISTANT ADMINISTRATOR FOR GRANT PROGRAMS OF THE FEDERAL EMERGENCY MANAGEMENT AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

NOVEMBER 9, 2007

Available via http://www.gpoaccess.gov/congress/index.html

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

38–983 PDF WASHINGTON : 2008

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
BARACK OBAMA, Illinois
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana

SUSAN M. COLLINS, Maine
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
PETE V. DOMENICI, New Mexico
JOHN WARNER, Virginia
JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*
KRISTINE V. LAM *Research Assistant*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
JENNIFER L. TARR, *Minority Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*

CONTENTS

	Page
Opening statements:	
Senator Lieberman	1
Prepared statements:	
Senator Warner	4
Senator Collins	19
Senator Akaka	19

WITNESSES

FRIDAY, NOVEMBER 9, 2007

Robert D. Jamison to be Under Secretary for National Protection and Programs, U.S. Department of Homeland Security	3
W. Ross Ashley III to be Assistant Administrator for Grant Programs of the Federal Emergency Management Agency, U.S. Department of Homeland Security	5

ALPHABETICAL LIST OF WITNESSES

Ashley, W. Ross III:	
Testimony	5
Prepared statement	109
Biographical and professional information	114
Responses to pre-hearing questions	123
Letter from U.S. Office of Government Ethics	160
Responses to post-hearing questions	161
Jamison, Robert D.:	
Testimony	3
Prepared statement	21
Biographical and professional information	25
Responses to pre-hearing questions	32
Letter from U.S. Office of Government Ethics	68
Responses to post-hearing questions	69

NOMINATIONS OF ROBERT D. JAMISON AND W. ROSS ASHLEY III

FRIDAY, NOVEMBER 9, 2007

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 9:07 a.m., in Room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senator Lieberman.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Good morning to everyone. Thanks for being here at this early hour, although probably I was up later than any of you last night because we were here voting until after 11 p.m.

We are here to consider nominees to two very important positions at the Department of Homeland Security. The first is Robert D. Jamison, who has been nominated to be Under Secretary of the Department of Homeland Security with responsibility for the National Protection and Programs Directorate (NPPD). Second is W. Ross Ashley III, nominated to be Assistant Administrator for FEMA in charge of Grant Programs.

Both of these jobs cover critical aspects of our homeland security, a wide range from cyber security to ensuring that our State and local partners have the resources they need on the front lines of our defense against all disasters, whether natural or man-made.

If confirmed, these two nominees before us today will have to work closely with our Nation's first responders, with the private sector, and with State and local officials to provide overall strategic guidance and support. I would say that as this Committee—from which the original proposal to create the Department of Homeland Security came—continues our oversight of the Department, I feel some satisfaction that we have made substantial progress in improving the capacity of the Federal Government to both prevent and respond to disasters, whether natural or terrorist. But I think we all agree that we have some way to go to get us to where we need to be in this threat environment. And it is in that cooperative spirit that I look forward to this hearing.

[The prepared statement of Senator Lieberman follows:]

PREPARED STATEMENT OF SENATOR LIEBERMAN

Thank you all for coming today. We are here to consider nominees to two important positions at the Department of Homeland Security. The first is Robert D. Jamison, who has been nominated to be Under Secretary of DHS, with responsibility for the National Protection and Programs Directorate (NPPD), followed by W. Ross Ashley III, nominated to be Assistant Administrator for FEMA in charge of grant programs.

Both jobs cover critical aspects of our homeland security from cyber security to ensuring that our State and local partners have the resources they need on the front lines of our defense against all disasters, whether natural or man-made.

The post Mr. Jamison has been nominated to is relatively new and consists of a medley of responsibilities, including cyber security, infrastructure protection, foreign traveler screening, emergency communications, and risk analysis.

I have several concerns that I'd like to discuss with Mr. Jamison. The Department continues to work with the private sector to ensure risk assessments are performed for the Nation's most critical infrastructure, although, we are behind in this effort. The process must be sped up as experience tells us terrorists are likely to target large structures and systems that will cause maximum havoc.

The Department must also move ahead expeditiously with the new chemical site security program, and must ensure that the program is sufficiently rigorous to significantly reduce this homeland security vulnerability.

The Office of Infrastructure Protection is heavily dependent upon outside contractors. Half the office staff is made up of contractors. As a matter of fact, 42 percent of the grants program directorate is also made up of contractors—and they are performing key functions like helping figure out the methodology by which we allocate grants. The Government Accountability Office recently testified before this Committee that overdependence on contractors deprives the government of the institutional knowledge it needs to perform its functions over the long run. I will want to know how Mr. Jamison and Mr. Ashley plan to prevent this from happening within their areas of authority at DHS.

We also face serious challenges protecting government computer systems and databases, another area that will fall within Mr. Jamison's portfolio. With persistent vacancies in key positions, and all too frequent reports of missing computers and lost equipment, everyone agrees we have not made sufficient progress, given the threats that exist to our cyber systems.

I am pleased, however, that the Department is now busy working on how to address many of these cyber security problems in a coordinated way. Just this week, the Administration announced its new Cyber Initiative to strengthen the protection of all government systems and databases. The program is still under development, and of course much about it remains classified, but I look forward to hearing as much detail as can be discussed in a public setting.

The position to which Mr. Ashley has been nominated—Assistant FEMA Administrator, heading the Grant Programs Directorate—is of special interest to me for a couple of reasons. I have made it a point over the past 4 years to work as hard as I could to obtain extra funding for our under-trained and under-equipped police officers, firefighters, and emergency medical workers who are on the front lines of the disasters that strike American communities.

In February, for the fourth year in a row, the President's FY 2008 budget request for the Department of Homeland Security would have cut crucial support for these brave men and women—slashing overall homeland security grant funding by a staggering 40 percent. That is unconscionable to me and would have been tantamount to disarming in the middle of a war. I hope you recognize the ongoing needs of first responders, Mr. Ashley, and I look forward to hearing your views on grant budgeting.

I am also keenly interested in grants because of legislation we passed earlier this year to fulfill most of the remaining 9/11 Commission recommendations. That measure, now signed into law, calls for substantial funding increases for training, planning, and new equipment for first responders.

Furthermore, we finally settled a year-long dispute over how to dispense homeland security grants in a way that would provide even more anti-terrorism funding on the basis of risk, while giving each State a smaller percentage of guaranteed funding for some basic level of preparedness. We also authorized more funding for key programs designed to help all States prepare for natural disasters and other threats.

Implementation of this provision is very important to me, Mr. Ashley, so I look forward to hearing your plans.

If confirmed, these two nominees before us today will have to work closely with our Nation's first responders, with the private sector, and with State and local officials to provide overall strategic guidance. We have made important strides, but still have much to do to protect our critical infrastructure, while also preparing ourselves for the next disaster that inevitably will come. Thank you.

Senator LIBERMAN. I will have several questions to ask after you make your opening statements, which I hope will allow us to have a conversation about some of those issues.

Both nominees have filed responses to a biographical and financial questionnaire. They have answered pre-hearing questions submitted by the Committee and had their financial statements reviewed by the Office of Government Ethics. Without objection, this information will be made a part of the hearing record with the exception of the financial data, which are on file and available for public inspection in the Committee offices.

Our Committee rules require that all witnesses at nomination hearings give their testimony under oath. Mr. Jamison and Mr. Ashley, would you please stand and raise your right hand?

Do you swear that the testimony you are about to give to the Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. JAMISON. I do.

Mr. ASHLEY. I do.

Chairman LIEBERMAN. Thank you. Please be seated.

We will begin with Mr. Jamison. I understand you have family here with you today, and I would be delighted to have you introduce them to us, and then proceed with your statement.

Mr. JAMISON. Thank you, Mr. Chairman. My wife, Meg, and my daughters, Elizabeth and Caroline, are here. I would like to thank them for their support not only today but every day leading up to it.

Chairman LIEBERMAN. You know, all the tough questions I had prepared, looking at those two adorable girls, I think I am just going to throw them out. [Laughter.]

Mr. JAMISON. Thank you, sir.

Chairman LIEBERMAN. Go right ahead.

TESTIMONY OF ROBERT D. JAMISON,[1] TO BE UNDER SECRETARY FOR NATIONAL PROTECTION AND PROGRAMS, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. JAMISON. Mr. Chairman, thank you for the opportunity to appear before you today. I am very grateful to President Bush and Secretary Chertoff for their confidence in my ability to lead the National Protection and Programs Directorate. I believe in the missions of the Department of Homeland Security and the Directorate and know they are critical to our Nation's security.

Serving in the Federal Government with thousands of people who take part in the many different aspects of securing the Nation, its people, and its critical assets and systems has been an honor. I appreciate the opportunity I have had in the past few weeks to communicate with the Committee about my professional experience and work that I have done in the public, private, and not-for-profit sectors.

[1] The prepared statement of Mr. Jamison appears in the Appendix on page 21.

In my roles at the Department of Transportation and the Department of Homeland Security, as well as in my positions at the American Red Cross and United Parcel Service, I have relied on three fundamental principles that I learned very early in my career: Have a commitment to attract and retain skilled people, focus on outcome-based results, and instill and insist on a culture of accountability and integrity. Those are the fundamentals I have focused on since I was named Deputy Under Secretary of NPPD in April, and those are the fundamentals I will continue to pursue if confirmed.

NPPD is a diverse organization with an important cross-cutting, binding mission of risk reduction. I believe in the mission and, if confirmed, would continue to strive for improvement.

I know that you and many of the Members have concerns about the stability of the Directorate and question if we are prepared for a transition of administrations. I firmly believe that an overarching goal for the Directorate must be its successful growth and stabilization. For that reason, the maturation of the Directorate must be a top priority that I will continue to pursue if confirmed.

One issue with relevance to maturing the Directorate is NPPD's use of contractor staff. As we evaluate this usage and convert contract staff to full-time Federal staff where appropriate, we will strike the balance that makes the Directorate more efficient and ensures that we have the skills necessary to position the Directorate for future success.

NPPD's broad and important portfolio demands dedicated stewardship. If confirmed, I would commit to strengthening an organization that works closely with the Department's security partners and stakeholders across the country. NPPD would also continue to be an organization that respects and relies on the direction and guidance provided by the Administration and Congress. If confirmed, I intend to work closely with and draw from all the individuals and entities able to assist the Directorate in fulfilling its mission.

I believe that NPPD, in addition to having a critical mission, is the right place to serve for those who are highly skilled, highly motivated, and profoundly dedicated to the security of our Nation. If confirmed, I will be proud to serve alongside the men and women of NPPD. Thank you.

Chairman LIEBERMAN. Thanks very much, Mr. Jamison, for that opening statement. I appreciate what you said.

Mr. Ashley, I want to note for the record that Senator John Warner, our dear friend and colleague from Virginia, had hoped to be here to introduce you this morning but had a scheduling conflict and is unable to be here. Senator Warner has submitted a statement of introduction and, I might say, great praise, and without objection, we will place it in the record.

[The prepared statement of Senator Warner follows:]

PREPARED STATEMENT OF SENATOR WARNER

Chairman Lieberman, Senator Collins, and my other distinguished colleagues on the Senate's Homeland Security and Governmental Affairs Committee, I thank you for holding this confirmation hearing today.

Today, I am pleased to introduce a Virginian, Ross Ashley, who has been nominated to serve as the Assistant Administrator for Grant Programs, Federal Emer-

gency Management Agency, Department of Homeland Security. He is joined today with his family including his wife, Lauren, his daughter, Catherine, his sons Cailan and Patrick, his mother, Brenda Dumas, and his brother Major John Ashley. I understand that his youngest daughter, Caroline, is not here today.

Mr. Ashley graduated from Tabb High School in Yorktown, Virginia, and subsequently earned his B.A. degree in International Studies from George Mason University in 1989 and M.S. in Strategic Intelligence from the Joint Military Intelligence College. From 1997 to 2004, Mr. Ashley served in the Air Force Reserves as an Intelligence Officer. He retired at the rank of Captain. In addition, from 1984 to 1997, Mr. Ashley served in the Virginia Air National Guard in Richmond, Virginia. Mr. Ashley has received numerous accolades for his military service.

The job of Assistant Administrator for Federal Grant Programs is a critical one, tasked with responsibility of overseeing a comprehensive assortment of grant programs at FEMA ranging from funding for communications equipment for first responders to funding for the hiring of firefighters. Due to the breadth of FEMA's grant programs, this job requires an individual with significant involvement in executing complex grant programs. Mr. Ashley has past work experience advising entities participating in the Federal grant process.

Mr. Ashley has almost 20 years of experience and expertise as an officer or executive at a diverse set of companies ranging from a non-profit provider of services to individuals with disabilities to high-tech companies. Through his various positions, including Director of Law Enforcement Technologies at ISX Corporation and as President and Chief Operating Officer at The Templar Corporation, Mr. Ashley has concentrated his work on information operations, strategic planning and execution, strategy assessment, operations analysis, team development, and project management which are all areas of critical expertise for a grant program administrator.

I am pleased to introduce Mr. Ashley today and I urge the Committee to give him every appropriate consideration.

Chairman LIEBERMAN. Mr. Ashley, I believe you have some family here also. We would welcome their introduction and then your opening statement.

Mr. ASHLEY. First off, my wife, Lauren, is here; my son, Cailan; daughter, Catherine; and our other son, Patrick. We also have a 2-year-old, Caroline, that we thought best not to be here today.

Chairman LIEBERMAN. Am I getting older or are the nominees getting younger? [Laughter.]

Mr. ASHLEY. My mother, Brenda Dumas, is also here visiting from Alabama.

Chairman LIEBERMAN. That is great.

Mr. ASHLEY. My brother, Major John Ashley; my sister-in-law; and aunt- and uncle-in-law and cousin-in-law are here as well.

Chairman LIEBERMAN. That is great. I cannot resist one of my favorite one-liners, which is that somebody, noting the presence of your mother-in-law, somebody said to me when they met my mother-in-law, which is that behind every successful man, there is a surprised mother-in-law. [Laughter.]

Apparently your mother-in-law agrees with that.

Mr. ASHLEY. "Shocked" might be appropriate.

Chairman LIEBERMAN. OK, Mr. Ashley, go right ahead.

TESTIMONY OF W. ROSS ASHLEY III[1] TO BE ASSISTANT ADMINISTRATOR FOR GRANT PROGRAMS OF THE FEDERAL EMERGENCY MANAGEMENT AGENCY, U.S. DEPARTMENT HOMELAND SECURITY

Mr. ASHLEY. Good morning, Mr. Chairman. My name is Ross Ashley, and I would like to thank Senator Warner for his statement of support as well.

[1] The prepared statement of Mr. Ashley appears in the Appendix on page 109.

I am appearing before you today as the nominee for Assistant Administrator for Grant Programs at the Federal Emergency Management Agency within the Department of Homeland Security. It is a great honor to be nominated by the President for this position and to have the opportunity to answer the questions as you consider my nomination. I cannot express how honored I am to be nominated for a position that will continue to further preparedness, response, and recovery capabilities of our State, local, and tribal partners and of our Nation as a whole.

I would like to begin today by thanking my wife, Lauren, for her patience and encouragement over the last 10 years as our family has grown. As each of you know, public service requires dedication and commitment from the whole family.

Also with us today are our oldest daughter and two sons—Catherine, Cailan, and Patrick—who inspire me with the eagerness with which they approach the start of every day. Our 2-year-old daughter, Caroline, thought best to hold down the fort while the rest of the family came to the hearing today. My mother is here from Alabama, and I would like to thank her for making the trip to be with us.

I have had the privilege of growing up in a family full of public servants. My father retired from serving both in the U.S. Air Force and the National Guard, and my mother worked in rural Mississippi as a social worker. My brother, Major John Ashley, is here today from serving on active duty in the National Guard. John is the true picture of the citizen soldier, having piloted F–16s on multiple combat deployments to Iraq and now preparing himself and others for deployment again in a new theater-based reconnaissance aircraft. John, his wife, Tracy, and their four children's dedication to their country is an inspiration to all of us who know them.

If confirmed as Assistant Administrator for Grant Programs, my responsibility will be to ensure that Federal investment into State, local, and tribal preparedness, response, and recovery capabilities provides the greatest return on investment for the American public. I will bring to this position many years of experience of military service, financial management, and executive leadership. I spent 20 years in the National Guard and Reserves, serving both as an enlisted member and as a commissioned officer. Early in my National Guard career, I volunteered on a number of occasions to fill sandbags and to pre-position supplies and equipment in order to prepare for hurricanes and floods threatening the Commonwealth of Virginia. Immediately following September 11, 2001, as a reserve officer I volunteered to augment active-duty personnel at the Pentagon, manning a 24-hour intelligence watch center.

From the time I was 18 years old, the educational and professional opportunities afforded me in the National Guard have been the foundation for every endeavor in my life, and if confirmed, I will bring this foundation with me to this new challenge.

One of the most important aspects of this position is to ensure that Federal investments and partnerships with State, local, and tribal first responders provide support to meet the National Preparedness Guidelines and the Target Capabilities List. This process requires financial experience in grant programs, fiscal responsibility, and accountability.

Since 1997, I have had the opportunity to work as a commercial partner with State, local, and tribal first responders, specifically in the areas of information sharing, incident management, and communications interoperability. As the founder and president of the Templar Corporation, I worked with individual States and localities on regional information sharing grants and supported all aspects of the grants process, from interpretation of guidance, preparation of submission packages, and financial and programmatic compliance. If confirmed, I believe I will bring the necessary perspective of our State, local, and tribal partners to the execution of all grant programs.

Prior to September 11, 2001, I supported the initial efforts to provide regional interoperable capabilities to our Nation's first responders. Shortly after the killing of Gianni Versace in 1997, it was discovered that his killer, Andrew Cunanan, pawned property under his real name while there was a nationwide manhunt underway for his apprehension. As a result of this and other multijurisdictional events, I worked with the Department of Justice and other partners to develop a real-time distributed information-sharing system for Broward, Brevard, and Monroe Counties in South Florida. Since these early efforts, I have had the opportunity to support similar interoperability efforts for both voice and data communications in a number of States and multi-jurisdictional regions, to include the National Capital Region.

My financial management experience includes efforts with my business partner to mortgage our houses and start a successful small business, participating in complex multi-million-dollar corporate sales in both the commercial and nonprofit sectors, and leading a high-performance financial management team in the turn-around of a challenged nonprofit.

As the CEO of an 1,100-person nonprofit, I was responsible for multiple cost centers and funding agencies at both the State and Federal levels that cut across all aspects of the lives of people with developmental disabilities. When I took over as CEO of the National Children's Center, the previous year audit included 32 findings of significant deficiency. Working with and leading a great team, we were able to, in one short year, reduce the number of auditing findings to two, neither of which was in the area of financial management.

It is also critical at this point to ensure that the resulting organizational changes in grant programs have a minimum effect on our stakeholders. Over the years, working with States and localities, one of the common themes in grant programs is the need for consistency year over year. If confirmed, I will ensure that the transition to a one-stop shop for grant programs continues to fully support all of our stakeholders. In addition, if confirmed, I am committed to an effective transition to the next Administration and will ensure that my successor has all the tools necessary to continue the tremendous work already accomplished by this Congress and the Administration.

Our Nation's grant programs are critical to ensure adequate all-hazard planning and operational capabilities for emergency managers, firefighters, law enforcement, medical response, and everyday citizens. If confirmed, I look forward to working with Adminis-

trator Paulison, the FEMA leadership team, across the Department of Homeland Security, and with all of our partners, continuing the efforts to develop a new FEMA and a culture of preparedness across our society.

In closing, the Congress continues to support the efforts of our Nation's first responders and has provided the necessary guidelines in the Post-Katrina Emergency Reform Act of 2006 and the Implementing Recommendations of the 9/11 Commission Act. If confirmed, I welcome the opportunity to continue these efforts to support our Nation's first responders and respectfully ask this Committee to confirm my nomination to serve as Assistant Administrator for Grant Programs at the Federal Emergency Management Agency within the Department of Homeland Security.

I want to thank you, Mr. Chairman, for the opportunity to appear before you, and I would be happy to answer any questions you may have.

Chairman LIEBERMAN. Thanks very much, Mr. Ashley.

I am going to start my questioning with the standard questions we ask of all nominees, and in the interest of efficiency, I will ask them of both of you simultaneously.

Is there anything you are aware of in your background that might present a conflict of interest with the duties of the office to which you have been nominated?

Mr. JAMISON. No.

Mr. ASHLEY. No, sir.

Chairman LIEBERMAN. Thank you. Do you know of anything, personal or otherwise, that would in any way prevent you from fully and honorably discharging the responsibilities of the office to which you have been nominated?

Mr. JAMISON. No.

Mr. ASHLEY. No, sir.

Chairman LIEBERMAN. And, finally, do you agree without reservation to respond to any reasonable summons to appear and testify before any duly constituted committee of Congress if you are confirmed?

Mr. JAMISON. I do.

Mr. ASHLEY. Yes, sir.

Chairman LIEBERMAN. Thank you very much.

Mr. Jamison, I think what I will do is go back and forth, one question to each. Let me begin with the Cyber Security Initiative, which is a very important part of the new world of attack and defense.

On Tuesday of this week, President Bush sent to Congress an amendment to the fiscal year 2008 budget request, reallocating funds to protect Federal civilian agency networks. This change is part of a new governmentwide effort on cyber security called, as you know, the Cyber Initiative. The request includes an increase of $115 million for cyber security within the NPPD at the U.S. Computer Emergency Readiness Team, also known as US–CERT. This increase would more than double the current budget of the Department for cyber security.

I wanted to ask you whether you believe this new initiative will fundamentally alter the approach that the Department has taken toward cyber security, and in answering that question to the best

of your ability, tell us what you think are the current capabilities of the Department relating to cyber security. And I would say that I understand that certain parts of the program are classified, and I respect that. But also I understand that many details are unclassified, and I would like you to speak from that base of information.

Mr. JAMISON. Yes, sir. First of all, I do believe this is a fundamentally new approach, but I believe it builds upon the capabilities that we have in US–CERT. US–CERT has a 24-by-7 response capability and provides a valuable service to respond and analyze the threat environment. And I must say that we at DHS, as well as in the Administration, are very concerned about the cyber threat and the fact that attacks are more prevalent, more focused, and more sophisticated. And as a result——

Chairman LIEBERMAN. We are seeing such attacks, aren't we?

Mr. JAMISON. Yes, we are.

Chairman LIEBERMAN. Yes.

Mr. JAMISON. And they are more frequent. And as a result, we have an interagency effort that is looking differently at cyber security.

But our approach and the role that DHS is going to play in that is really a more aggressive approach to some of the current capabilities that we have most fundamentally. Currently, we have a capability to do intrusion detection with an Einstein Program. We want to get much more aggressive and ramp that out across the Federal Government. We also want to look at how we are managing the security policies and standards across the Federal Government, and US–CERT will play a much more prominent role in that.

But it really builds on fundamental capabilities. I cannot say enough about the technical expertise that we have in US–CERT, and this initiative will dramatically ramp up that capability, add more staff to do more analysis of threats and allow us to respond as a government comprehensively, and have us have better situational awareness on what is happening across the dot-gov network.

I would be very happy, as we have done with your staff, to give you a detailed classified briefing on some of the classified parts of that initiative. But to reiterate your first point of the question, I do think it is a fundamentally different approach, but it builds on our current capabilities.

Chairman LIEBERMAN. I appreciate it, and I would like to do that. Let me ask you one related question. Given that the majority of the cyber infrastructure is owned privately by industry, will this initiative also help monitor and protect those systems?

Mr. JAMISON. What we are talking about in the Cyber Initiative for 2008 is focused on the dot-gov network.

Chairman LIEBERMAN. Right.

Mr. JAMISON. But just as we saw recently with the visibility that the control system vulnerability got in the U.S. that we have been working on at DHS with our interagency partners and with the public-private partnership, we must not forget about the vulnerabilities to our critical infrastructure and the threat that exists in the cyber domain. So we are going to continue to work those partnerships just like we have through the NIP Partnership

Framework, continue to roll out mitigation measures, and to look at that.

But the main focus of the Cyber Initiative is to focus in 2008 on the dot-gov networks and try to get more secure in that area.

Chairman LIEBERMAN. Good.

Mr. Ashley, let me ask you a couple of questions related to the Federal Government's attempt to enhance terrorism prevention efforts at the State and local level. The National Strategy for Homeland Security says that "State, local, and tribal governments which best understand their communities, will always play a prominent front-line role in helping to prevent terrorist attacks." And I could not agree more.

Could you describe what steps you will take to ensure that State and local law enforcement are full partners in national prevention efforts to defeat Islamist terrorism which the Department and the FBI have identified as the greatest threat to the homeland?

Mr. ASHLEY. Yes, sir. I agree wholeheartedly with your statement there as far as the people on the ground that understand best our communities are State, local, and tribal first responders. The efforts that will continue to make a big difference in this area are cross-discipline fusion centers for the law enforcement community. And when I say cross-discipline, I am also including the rest of the first responder community there because I think it is very important for the continued efforts of preparedness planning to look across all disciplines, be it emergency managers, firefighters, law enforcement, or medical response.

Continuing those planning initiatives, many people say that planning is critical and the plan is worthless. I think that as we enhance the fusion center efforts and as we enhance planning capabilities across disciplines, this will begin to break down some of those barriers and allow people to start sharing information across these disciplines.

Chairman LIEBERMAN. That is very important. Let me go to a different part of it. This Committee held a hearing last week—a very important hearing to me, and I think to the Committee—in which local police officers from New York, Los Angeles, Kansas City, and Miami-Dade County testified about the importance of outreach and forging bonds with local Muslim-American communities that are essential in preventing the spread of Islamist radicalization and extremism. But they all testified that they have not yet been able to use their homeland security grants for such efforts.

The Implementing Recommendations of the 9/11 Commission Act, as we call it, provides the FEMA Administrator flexibility to allow State and local communities to spend homeland security grants on "any appropriate activity" relating to preventing, preparing for, protecting against, and responding to acts of terrorism.

Will you indicate to us that you are going to do what you can to ensure that the upcoming grant guidance will authorize the use of grants by State, county, and local law enforcement for the kind of community outreach that I have talked about?

Mr. ASHLEY. Of course, I am not aware of what is currently written in the fiscal year 2008 grant guidance. However, I will tell you that I think it is critical that outreach is conducted by State and

local partners, and I meant that in many different ways, whether it is reaching out to a local Muslim community or whether that is reaching out to the commercial businesses that may have assets that are required and such like that. Also, from the standpoint of privacy, as we begin to stand up these fusion centers across the country, I think it is critical that community buy in to the process so there is not this vision of a green door that the community is unaware of what is going on. So I am committed to working with Administrator Paulison and expressing those, if confirmed for the position, yes, sir.

Chairman LIEBERMAN. I appreciate that. To say what you know, the 750,000 county, State, and local law enforcement people around the country, they are really a mighty force to implement everything we are trying to do at the Federal level to detect and prevent and, God forbid, have to respond to a terrorist attack. They seem quite ready to get at this. I was impressed last week that these four departments took this initiative on their own, and right now they are supporting it entirely, as far as I can determine, through locally generated revenues.

There are, in fact, in my staff's investigation of this matter, some police departments in communities that have significant Muslim-American communities that are not doing any of this outreach, and we will talk about that. But I hope that you can both urge and support them getting involved in it.

Do you have any thoughts about how you might more broadly involve other first responders? I am thinking particularly of firefighters and emergency medical personnel.

Mr. ASHLEY. Sure. I think that one of the things that you all envisioned in this Congress when it came to putting grants all into one location is one of the expectations is that we would look across all of those grant programs to ensure the best possible preparedness. I think there is an opportunity now, with the grants being in a consolidated, one-stop-shopping environment, to begin looking at the guidance as it goes across disciplines and to continue to encourage things like the Regional Transit Working Group's participation on the UASI programs and that cross-discipline planning and coordination.

As far as bringing the law enforcement and emergency managers group together, again, as we start standing up these fusion centers, we have the opportunity to write into grant guidance how those relationships will interact with emergency management centers across the country. A lot of this is unwritten and new at this point, and there are a lot of new cultural barriers that are beginning to come down at the grass-roots level. And I think that by doing that at the Federal level, by putting everything in the same department, it also gives us an opportunity to organize inside of the Grant Programs Directorate, so there is that cross-pollination across those grant programs, whether it is firefighters, emergency managers, law enforcement, or medical response.

Chairman LIEBERMAN. I agree. You are coming on at an important time at the beginning of this reorganized function to make it work, so I appreciate that.

Mr. Jamison, let me go back to you. Earlier this year, as you well know, DHS alerted many sectors to a vulnerability known as the

Aurora scenario, which showed that rotating electrical machines used throughout critical infrastructure could be damaged through a remote cyber attack. This vulnerability, which poses a severe potential impact for many industries, including electric, nuclear, and water, illustrates the even greater potential risk that exists due to increasing interconnectivity between more traditional systems and the Internet. So let me ask you a few questions about that.

First, do you believe that particular risk has been mitigated?

Mr. JAMISON. I believe we have taken a lot of risk off the table, and I think it is a good example of how the NIP Partnership Framework worked with our industry partners and our Federal agency partners to quickly—once our research had indicated there was a vulnerability, to work to develop mitigation measures and to roll those out. We need to continue to monitor the performance in the field on the implementation of those mitigation measures, but we started with our high-risk infrastructure and are confident that the industry and the sectors are taking action as necessary.

Chairman LIEBERMAN. As you probably know, some members of the impacted sectors said that DHS did not notify them of this Aurora vulnerability in a timely or consistent manner and failed to use the so-called Sector Coordinating Councils to disseminate information and seek counsel from sector experts. I know you know about this complaint. What did you learn from the Aurora scenario in terms of private sector coordination?

Mr. JAMISON. Sir, I am not familiar with that particular complaint. I think it may be due to the fact that we did risk analysis on the vulnerabilities across the sectors, and we engaged with certain sectors prior to other sectors.

I think what it proved to me is that the Sector Coordinating Council and the partnership that we have is a viable model to look at managing risk in a system where 85 percent of our infrastructure is owned by the private sector. Within a matter of months, once the vulnerability was verified, we quickly had mitigation measures in both the nuclear and the electrical sector and worked and had already started getting those mitigation measures out. We are continuing to work through the rest of those sectors. Several other sectors have engaged—I think it works. I think we need to continue to build upon that partnership and make sure that we strive to figure out better ways to continue to share sensitive information down to the people that need to have it in order to make the decisions and implement the measures. But it proved to me we have a framework that has come a long way over the last few years. We just need to continue to get better at using it.

Chairman LIEBERMAN. Do you think that DHS has adequate regulatory authority to ensure that the mitigation measures you have just talked about are being put into place throughout the critical infrastructure?

Mr. JAMISON. I am satisfied with our current authorities. I think we need to continue to make sure that we are doing outcome performance measures in the field to determine whether or not those mitigation measures are being implemented. And if we do not think that they are being implemented sufficiently, we either need to leverage the regulatory authorities or our partners, other agencies within the Federal Government, or ask for them like we did

in chemical security where we asked for additional regulatory authority when we thought we needed it. But the key is to make sure we carefully monitor the results.

One point I wanted to make about that vulnerability is that, for the most part, a lot of mitigation measures are low-cost investments that could protect high-risk, expensive pieces of equipment. And it is in the owner's best interest to take those mitigation measures from a capital protection standpoint. It is one of the reasons we are pleased with the results so far about the mitigation measures. But it is something we need to continue to look at and monitor.

Chairman LIEBERMAN. I agree. Good.

Mr. Ashley, we have talked a little bit about the Fusion Centers. One of the problems that State and local officials who have come before our Committee have identified with regard to the development of the Fusion Centers is that there is no guarantee of funding for long-term sustainment. And the problem, obviously, is that to work, they need to make long-term investments in technology and even training and personnel.

How will you work to assure the States that the Department remains committed to the Fusion Center program and that the grants that they depend on for these long-term investments will be there and will not suddenly disappear?

Mr. ASHLEY. Right. Planning from year to year and consistency from year to year has been a common theme with our State and local partners. I think one of the best ways to address this from a grant programs perspective is to work from the programmatic side to ensure State and locals are making investments that have deliverable milestones and leave-behind capability because at any given moment we do not know where the budget process is going to be with next year's funds, and etc., for State and local. So working with them to ensure that each year that they are investing grant dollars, that if they are working toward a longer-term goal, that there is leave-behind at each milestone. And that is, I will bring experience and program management to helping to support that process.

But it is a multi-year effort on many of these different issues, and we are reliant upon multiple moving parts to ensure year-over-year consistent funding.

Chairman LIEBERMAN. I hear it. Part of it is us. So the Committee will work very hard to assure that long-term sustainment as well.

Mr. Jamison, you mentioned a little bit about contracting in your opening statement. As you know, the Committee held a hearing last month that raised serious concerns about the Department's reliance on outside contractors to do the government's work. Overuse of contractors, obviously, we are concerned raises the risk that the Department itself is not developing the institutional knowledge for the longer term and, at worst, will lose control of its own decision-making. The problem appears to be significant in the NPPD. Half of the staff of the Office of Infrastructure Protection are contractors; for instance, three-quarters of the positions in the National Cyber Security Division were contracted out.

So I want you to describe a bit more—I know you have this under review—what actions you hope to take to reduce NPPD's reliance on contractors and really in a fundamental way how you intend to prepare the Directorate for the upcoming transition.

Mr. JAMISON. Yes, sir. I agree with you. I think that making sure that we have in-house Federal staff that can position ourselves for the transition and for the challenges that we face is absolutely crucial. Not only that, we need to make sure that we put a focus on retaining the key Federal staff that we currently have. So that is one of the reasons attracting and retaining the key people is a top priority for myself.

I have asked that a review be done to determine in 2008, given as contracts expire and given our capabilities to hire people, how many contractor staff should be converted to full-time Federal staff if appropriate for efficiency and appropriate for roles and responsibilities. We have a preliminary target for fiscal year 2008 to convert 150 staff from contractors to full-time.

Chairman LIEBERMAN. Good.

Mr. JAMISON. And I think most people that know me would tell you that I am an outcome-focused metrics type of person, and that is going to be one of my metrics for 2008 to make sure that we do that because I do believe it is a fundamental key point to make sure that we are more stable going into the transition.

Chairman LIEBERMAN. Good. We will obviously want to keep in touch with you on all that.

Mr. Jamison, when Congress passed the Post-Katrina Emergency Management Reform Act over a year ago, we created the Office of Emergency Communications (OEC). As you know, DHS was supposed to submit a report to Congress within 120 days of enacting the law outlining the resources needed to establish the office.

The Committee just received the report this week, and obviously we are grateful for that, but also concerned that OEC is not as far along as we hoped it would be at this point. And there are other deadlines, as you may know, that OEC also has to meet.

Could you update the Committee, to the best of your knowledge at this point, on the status of the Office of Emergency Communications?

Mr. JAMISON. Yes, sir. First of all, we have faced some challenges in the stand-up of OEC, standing up a new organization and making sure that we have the staff in place and the leadership in place to move forward. I am glad we got the report up here this week. I think it is representative of the resources that we need and an alignment of where we need to focus our resources. But more importantly, over the last few months we have named a Deputy Director that has a long history of emergency communications in the field, in working with State and locals and being a part of that emergency responder community that is going to bring a lot of experience to that. He has been on board for, I think, about 6 weeks now. We are in the final processes of bringing on board, offers have been accepted, another—the director of that office, who also brings valuable State emergency communications experience. Those are the two biggest pieces to the puzzle, in my opinion, to taking this organization to the next level. Do we need to get better at our reporting timeliness? Yes. Do we have the pieces in place to start

moving forward? Yes. I think we have come a long way in the last year, but we need to make sure we are building on that foundation.

Chairman LIEBERMAN. OK. That is hopeful.

And this one is to you, Mr. Ashley.

Mr. ASHLEY. OK.

Chairman LIEBERMAN. It is similar. Congress established the Interoperable Emergency Communications Grant Program when it passed the Implementing Recommendations of the 9/11 Commission Act. Funding for the new program was included in both the Senate and House homeland security appropriations bills, and we are really looking forward to the program beginning next year. This is, as you know, from a tragic real-life experience, both on September 11, 2001, in New York where we lost a lot of firefighters because of the inability to communicate with other first responders, and then when in Hurricane Katrina they just were not able to operate, let alone communicate.

So I wanted to ask you what steps the Department has taken and do you intend to take to get this critically important Interoperable Emergency Communications Grant Program up and running during fiscal year 2008?

Mr. ASHLEY. Yes, sir. There are a couple things there. We also have the PSIC grants as well that came out of Commerce, and ensuring that those grants are synergistic and working together, utilizing the same grant guidance.

Specifically, I think in what you guys accomplished with the 9/11 bill and the requirement of statewide interoperability plans being submitted and going and working with the Office of Emergency Communication and looking at those statewide plans and ensuring investment across interoperable communications efforts are done in a coordinated fashion, I think you guys have given us a lot of guidance in that area as well.

I think the utilization of the similar grant guidance from SAFECOM as far as both for PSIC and interoperable communications in my understanding as well is that we have individuals that are actually working in the Office of Emergency Communications as well to make sure there is that tight fit between the policy and the review of the statewide plans and then the implementation of grants. I think that the groundwork has already started to take place, and I look forward to working with Mr. Jamison to further that.

Chairman LIEBERMAN. Good. Obviously, we really want to see this up and running and beginning to turn to plug this gap during this coming fiscal year.

DHS announced earlier this year that it intends to direct the airlines to collect biometric information, including fingerprints, from international travelers in order to carry out the air exit requirement of the US–VISIT program. Mr. Jamison, I wanted to ask you what is the status of the proposal and whether you believe it is appropriate to delegate this immigration and law enforcement function to the private sector.

Mr. JAMISON. Yes, sir. Currently, we are in the late stages of drafting a Notice of Proposed Rulemaking. We want to have that out in the very near future with the goal of hopefully having the final rule implemented by this summer, June 2008, and with an

implementation date of December 2008, to actually start the biometric collection.

We are currently in the late stages of doing final cost/benefit analysis in preparation for that Notice of Proposed Rulemaking, but from a principles standpoint, we do believe that this is not inconsistent with the airlines' responsibility currently to collect passport information and other passenger information required for the government, and this will be consistent in that realm as well.

We need to make sure we carefully evaluate the true costs to the airlines versus the costs to the government of doing that function. But we do believe that is a function that can be carried out most effectively by the airlines.

Chairman LIEBERMAN. What impact do you think the proposal will have on passenger processing at airports?

Mr. JAMISON. It is something that we are taking into consideration very carefully. It really depends upon the point at which a biometric will be collected. Our current thinking is that the check-in counter is the most efficient place to do that.

Chairman LIEBERMAN. Right.

Mr. JAMISON. We do not think that it will have a big impact on line delays due to the other processing that takes place, and while the reservations are printing and tickets are printing, there is a capability because it is a very short transaction, a matter of, I think, about 20 seconds to do the full biometric collection. So we do not anticipate a full impact. We are carefully going through that evaluation in the Notice of Proposed Rulemaking to make sure that we have fully captured the impact to the airlines and to the wait times for the passengers.

Chairman LIEBERMAN. Are the airlines opposing that idea?

Mr. JAMISON. I think they will oppose that idea, and they have been fairly vocal about that.

Chairman LIEBERMAN. Right.

Mr. JAMISON. It becomes the issue, I think, that we have to determine where is the best place to do that and whether or not we really need that information in terms of knowing who is in the country.

Chairman LIEBERMAN. Obviously, we are finding pushback in a lot of different areas in which we are, in the interest of homeland security, asking people to do things that they have not done before, that they thought they would never have to do, but we are doing it for a reason. I know there will be pushback. There already has been. But in the end, we want you to be able to say that you have set up a system that will give maximum protection to the American people, even if some people are unhappy because they have to do a little more a little differently than they have done before.

DHS has reported that this whole change will be complicated and costly to the US–VISIT biometric exit system. Let me just ask you, finally, to step back and talk a little more about what you think the most significant challenges are in developing an exit system at land ports of entry. That is what I want to focus on for this question.

Mr. JAMISON. I think it is a significant challenge. As you know, at many of our border locations, we do not stop individuals from entering Canada at several border spots, so implementing an exit

regime in those land borders requires a significant challenge and significant resources.

I think that the process that we are about to embark on in air exit is going to inform us greatly on those challenges and at the same time will capture, I believe, about 94 percent of the visa waiver-eligible population that we are focused on capturing.

So that learning curve and going through that process will help us lay out the next phase of this and the strategy that is going to take us into the future years of getting a land exit program evaluated.

Chairman LIEBERMAN. OK. I thank both of you. You are obviously both very well informed and experienced to take on these critical assignments. These are two positions that the general public probably never has heard of and we hope, in a way, never does hear of. But what you are about to take on is critically important to the security of every person in this country and the country overall, the government overall. So I appreciate it very much. You both obviously have been blessed with devoted and beautiful families behind you, and as I think they know, you are going to need them to continue to be behind you in the time ahead, particularly your mother-in-law. [Laughter.]

I cannot tell you how important that is.

Without objection, the record will be kept open until 12 noon tomorrow for the submission of any written questions from Members of the Committee or statements for the record that you or others want to add. We are doing that very quick turn-around because it is my intention, based on the importance of these two positions, to bring your nominations before a Committee business meeting, which I believe is scheduled for next Wednesday, and then hopefully to move them through the full Senate quickly before we depart at the end of next week for our Thanksgiving two-week break. So be on good behavior between now and the end of next week. [Laughter.]

I thank you very much, and with that, the hearing is adjourned.

[Whereupon, at 9:54 a.m., the Committee was adjourned.]

APPENDIX

PREPARED STATEMENT OF SENATOR COLLINS

The nominations we consider today encompass two critical responsibilities at the Department of Homeland Security: management of the federal programs that protect our citizens from natural or man-made disasters, and administration of the grant programs that help States and localities improve their ability to counter terrorist attacks, respond to natural disasters, and communicate in emergencies.

The scope and importance of the NPPD's responsibilities are daunting. The NPPD is charged with:

- maintaining the Office of Bombing Prevention as a strong and active participant in the nation's efforts to counter the threat of terrorists using improvised explosive devices on our soil;
- ensuring successful implementation of the chemical-facility security program authorized last year, due to the work of this Committee;
- assessing risks and developing prioritized inventories of our nation's critical infrastructure, and
- managing voluntary private-sector coordination programs to achieve the goals of the National Infrastructure Protection Plan.

I would note that the Office of Bomb Prevention would be formally established and strengthened by the National Bombing Prevention Act that Senator Lieberman and I introduced last week.

The second nomination is to a position within FEMA that plays a vital role in preparing our State and local first responders to handle the next major natural disaster or terrorist attack.

The FEMA reform legislation that Senator Lieberman and I crafted in 2006 restored preparedness grant programs to FEMA. This improved the agency's ability to support State and local preparedness with funds for planning, training, exercises, and interoperable communications.

Grants are a vital part of our essential goal of achieving effective capabilities and coordination among federal, State, local, and other stakeholders in the preparation and response to natural disasters and terrorist attacks. As part of that effort, I would add, the Grant Programs Directorate has another critical role: ensuring that tax dollars are not wasted.

Ross Ashley comes before our Committee with a long record of executive experience in both commercial and non-profit organizations.

I join the Chairman in welcoming both of these nominees to this hearing.

PREPARED STATEMENT OF SENATOR AKAKA

I am pleased to join you today in welcoming Robert Jamison who has been nominated to serve as the Under Secretary of National Protection and Programs at DHS, and Ross Ashley, who has been nominated to serve as Deputy Administrator for Grant Programs at FEMA. These are important positions and their programs are essential to State and local governments trying to build effective disaster response capabilities.

Many States are still struggling with the need to upgrade or supplement outdated resources, including crowded emergency operations centers, to establish fusion centers for effective law enforcement and intelligence coordination, and to ensure that adequate surge capacity is available in the aftermath of a natural disaster or terrorist attack. DHS grants are a key resource in accomplishing those tasks.

Mr. Ashley, I cannot emphasize enough how important the effective and efficient administration of the grants process is to our State and local governments. It is my

hope that, during your tenure, you will communicate with those recipients *closely and often* to ensure that grant guidance is *clear, concise* and *easily understood.*

The threat of improvised explosive devices, protection of critical infrastructure and the possibility that our nation's power plants can be sabotaged because of vulnerabilities in cybersecurity are *no less critical* to the homeland security mission. I look forward to hearing how Mr. Jamison intends to move the NPPD from its recent establishment to a more mature directorate responsible for overseeing and implementing programs in those areas. I would also like to hear how the NPPD will work with State and local governments to not only ensure the security of critical infrastructure, but also its safety.

Senate Committee on Homeland Security and Governmental Affairs

Hearing on the Nomination of Robert D. Jamison to be Under Secretary for the National Protection and Programs Directorate, Department of Homeland Security

November 9, 2007

Mr. Chairman, Senator Collins, and distinguished Members of the Committee, thank you for the opportunity to appear before you today.

Let me begin by expressing my gratitude to President Bush and Secretary Chertoff for their confidence in my ability to lead the National Protection and Programs Directorate (NPPD). I believe in the missions of the Department of Homeland Security (DHS) and the Directorate and know they are critical to our Nation's security. I am honored to be considered as part of that effort.

I have had the privilege of serving in several posts in this administration. I served as Deputy Administrator of the Federal Transit Administration (FTA), overseeing an agency that supports locally planned and operated public mass transit systems throughout the United States. While at FTA, I was asked to fill in as Acting Administrator of the

Federal Railroad Administration, the agency charged with ensuring the safety of the Nation's railroad system.

Prior to my current position, I served as the Deputy Assistant Secretary of the Transportation Security Administration. It was an honor to serve with the more than fifty-thousand people who share the duty of ensuring the security of the Nation's transportation system. In addition to my Federal service, I have held leadership roles with the American Red Cross and United Parcel Service, where I enjoyed a thirteen-year career.

While most of my previous positions had the common underpinnings of transportation or logistics, the mission, operational structure, and business culture of each organization were quite different. I believe I was able to operate in those diverse environments effectively by relying on the fundamental principles I was taught early in my career. I worked to enhance my proficiency in applying these principles throughout my later assignments. Those fundamental principles are: have a commitment to attract and retain skilled people, focus on outcome-based results, and instill and insist on a culture of accountability and integrity.

Those are the fundamentals that I have focused on since I was named Deputy Under Secretary of NPPD in April. Those are the fundamentals I would continue to pursue if confirmed.

NPPD is a diverse organization with an important, cross-cutting, and unifying mission of risk reduction. The Directorate works to reduce risk in distinct mission areas, such as in the Office of Infrastructure Protection (OIP), which coordinates national efforts to reduce risk to our critical infrastructure and key resources. A top priority in OIP is the implementation of the recently developed chemical facility regulation regime. Concurrently, OIP must strive to continue to improve the security posture in all 17 critical infrastructure and key resource sectors. The Office of Cybersecurity and Communications is focused on reducing risk to the Nation's cyber network and maintaining the resilience of our communications systems. US-VISIT drives down risk by using biometric and biographic information to enhance the security of our citizens and visitors and to facilitate legitimate travel and trade. One of the most important keys to success is the continued collaboration and information sharing with our partners. NPPD plays lead roles in these areas as well as managing the Department's collaborative approach to quantify risk.

I believe that my background in the public and private sectors prepares me well to dedicate myself to NPPD's broad and important portfolio. My focus on accountability, outcome-based performance metrics, and reliance on the abilities and dedication of those working in the Directorate would guide my decisions and drive our risk-reduction

mission. Further, those principles would serve to support an environment where every individual clearly perceives how his or her work in the directorate contributes to fulfilling our mission, securing the homeland, and protecting its citizens.

If confirmed, I commit to strengthening an organization that works closely with the Department's security partners and stakeholders across the country. NPPD would also continue to be an organization that respects and relies on the direction and guidance provided by the Administration and by the Congress. For example, I have emphasized since my arrival at NPPD the importance of improving the function of the directorate through the recommendations offered by the Government Accountability Office and the Office of the Inspector General. I intend to work closely with and draw from all those individuals and entities to assist the Directorate in fulfilling its mission.

I believe that NPPD, in addition to having a critical mission, is the right place to serve for those who are highly skilled, highly motivated, and profoundly dedicated to the security of our Nation. If confirmed, I would be proud to serve alongside the men and women of NPPD.

BIOGRAPHICAL AND FINANCIAL INFORMATION REQUESTED OF NOMINEES

A. BIOGRAPHICAL INFORMATION

1. **Name:** (Include any former names used.)
   Robert Dewey Jamison

2. **Position to which nominated:**
   Under Secretary
   National Protection and Programs Directorate

3. **Date of nomination:**
   Tuesday, September 4, 2007

4. **Address:** (List current place of residence and office addresses.)

   Residence:

   REDACTED

   Office:
   3801 Nebraska Avenue, NW
   NAC Bldg 17 – 2nd Fl
   Washington, DC 20528

5. **Date and place of birth:**
   2/23/65
   Memphis, TN

6. **Marital status:** (Include maiden name of wife or husband's name.)
   Married
   Margaret Anne Riley-Jamison

7. **Names and ages of children:**

8. **Education:** List secondary and higher education institutions, dates attended, degree received and date degree granted.

   High School:
   Rossville Academy, 1979-1983, Diploma, Rossville, TN, 1983

   College:

University of Memphis (Memphis State University at the time), 1983-1987, BS, Electrical Engineering; Minor in Mathematics, 1987, Memphis, TN

9. **Employment record:** List all jobs held **since college, and any relevant or significant jobs held prior to that time**, including the title or description of job, name of employer, location of work, and dates of employment. (Please use separate attachment, if necessary.)

Department of Homeland Security 2005-Present
National Protection & Programs, Acting Under Secretary, 4/07 - present
National Protection & Programs, Deputy Under Secretary, 4/07 - present
Transportation Security Administration, Deputy Assistant Secretary, 10/05 - 4/07

Department of Transportation 2005-2002
Federal Railroad Administration, Acting Administrator, 1/05 – 6/05
Federal Transit Administration, Deputy Administrator 5/02 – 10/5

Expert Consultant 9/2001-5/2002
Federal Transit Administration

Unemployed 3/2000 – 9/ 2001
No active job search

American Red Cross 1997-2000
Senior Operations Officer, 6/99 – 3/2000
Vice President of Chapter Operations, 11/98 – 5/99
Chief Operations Analyst, 5-97 – 5/99

United Parcel Service
Facilities Engineering Manager, Burtonsville, MD, 2/95 – 5/97
Engineering Manager, Barcelona, Spain, 3/94 - 2/95
Building Manager, Harrisburg, PA, 10/90 – 3/94
Engineering Supervisor, Edison, NJ, 1/90 - 10/90
Project Engineer, Pinebrook, NY, 5/88 – 1/90
Part-time management, operations, and driver, Memphis, TN, 6/84 – 5/88

10. **Government experience:** List any advisory, consultative, honorary or other part-time service or positions with federal, State, or local governments, other than those listed above.
Expert Consultant 9/2001-5/2002
Federal Transit Administration

11. **Business relationships:** List all positions currently or formerly held as an officer, director, trustee, partner, proprietor, agent, representative, or consultant of any corporation, company, firm, partnership, or other business enterprise, educational or other institution.

N/A

12. **Memberships:** List all memberships, affiliations, or and offices currently or formerly held in professional, business, fraternal, scholarly, civic, public, charitable or other organizations.

Member of United Methodist Church of Collierville, Tennessee. I have not been an active member since moving from the area in 1988. However, I never ended or transferred my membership.
Member of the University of Memphis Alumni Association since 2002.

13. **Political affiliations and activities:**

(a) List all offices with a political party which you have held or any public office for which you have been a candidate.
N/A

(b) List all memberships and offices held in and services rendered to any political party or election committee during the last 10 years.
N/A

(c) Itemize all political contributions to any individual, campaign organization, political party, political action committee, or similar entity of $50 or more during the past 5 years.
10/25/2004 George W. Bush $1,000.00
10/12/2004 Republican National Cmte $500.00

14. **Honors and awards:** List all scholarships, fellowships, honorary degrees, honorary society memberships, military medals and any other special recognitions for outstanding service or achievements.

U.S. Department of Transportation Gold Medal, 2006
War on Terrorism Medal, U.S. Department of Transportation, 2004
President's Management Agenda "Champion", U.S. Department of Transportation, 2004
Secretary's 9/11 Medal, U.S Department of Transportation, 2003
American Red Cross Spirit of Excellence Award, 1999
Herff Scholarship (four-year, full tuition academic college scholarship)
Magna Cum Laude graduate of University of Memphis
High School Valedictorian

15. **Published writings:** Provide the Committee with two copies of any books, articles, reports, or other published materials which you have written.
N/A

16. **Speeches:**

(a) Provide the Committee with two copies of any formal speeches you have delivered during the last 5 years which you have copies of and are on topics relevant to the position for which you have been nominated. Provide copies of any testimony to Congress, or to any other legislative or administrative body.
Please see attached.

(b) Provide a list of all speeches and testimony you have delivered in the past 10 years, except for those the text of which you are providing to the Committee. Please provide a short description of the speech or testimony, its date of delivery, and the audience to whom you delivered it.
Please see attached.

17. **Selection:**

(a) Do you know why you were chosen for this nomination by the President?

I believe that the President nominated me for this position based on my past performance as Deputy Assistant Secretary for the Transportation Security Administration, as well as my understanding of the department and the challenges facing the National Protection and Programs Directorate. I also feel that my track record as Deputy Administrator for the Federal Transit Administration and Acting Administrator of the Federal Railroad Administration contributed to the decision to nominate.

(b) What do you believe in your background or employment experience affirmatively qualifies you for this particular appointment?

I have a broad range of management experience in the private, not-for-profit, and public sectors that I can bring to bear on the challenges facing the directorate. I have a proven track record of success across diverse operating environments which positions me well to address the multi-faceted challenges across the varied mission areas of the 17 Infrastructure Protection Sectors, the cross cutting domains of cyber security and communications, as well as the challenges in the directorate's other areas.

My operational experience from United Parcel Service has given me a solid business acumen foundation and a focus on accountability, outcome-based performance metrics, and efficiency.

On top of that business foundation, I have gained valuable operational management experience from the American Red Cross. The understanding of disaster relief operations complements my security experience and gives me a unique perspective into two critical areas involved in the important risk management and analysis work of the directorate.

At the Federal Transit Administration, I led process improvements to the oversight of large, complex, public transportation projects that resulted in

improved schedule and budget performance. My understanding and ability to instill strong project management, risk management, and good fiscal discipline into an organization will continue to benefit the directorate as we face many large scale deployment projects.

Additionally, my tenure at the Federal Railroad Administration coupled with my regulatory responsibilities at Transportation Security Administration (TSA) gives me valuable experience to leverage as the directorate rolls out the Chemical Facility Anti-Terrorism Standards and the continued development of the Office of Infrastructure Protection.

Finally, my tenure as the Deputy Assistant Secretary at TSA has given me tangible experience improving security across a complex and diverse operating spectrum. It also afforded me the opportunity to work closely with the private sector as well as our State and local partners to ensure collaboration and cooperation.

B. EMPLOYMENT RELATIONSHIPS

1. Will you sever all connections with your present employers, business firms, business associations or business organizations if you are confirmed by the Senate?
   N/A

2. Do you have any plans, commitments or agreements to pursue outside employment, with or without compensation, during your service with the government? If so, explain.
   No.

3. Do you have any plans, commitments or agreements after completing government service to resume employment, affiliation or practice with your previous employer, business firm, association or organization, or to start employment with any other entity?
   No.

4. Has anybody made a commitment to employ your services in any capacity after you leave government service?
   No.

5. If confirmed, do you expect to serve out your full term or until the next Presidential election, whichever is applicable?
   Yes.

6. Have you ever been asked by an employer to leave a job or otherwise left a job on a non-voluntary basis? If so, please explain.
No.

C. POTENTIAL CONFLICTS OF INTEREST

1. Describe any business relationship, dealing or financial transaction which you have had during the last 10 years, whether for yourself, on behalf of a client, or acting as an agent, that could in any way constitute or result in a possible conflict of interest in the position to which you have been nominated.
None.

2. Describe any activity during the past 10 years in which you have engaged for the purpose of directly or indirectly influencing the passage, defeat or modification of any legislation or affecting the administration or execution of law or public policy, other than while in a federal government capacity.
None.

3. Do you agree to have written opinions provided to the Committee by the designated agency ethics officer of the agency to which you are nominated and by the Office of Government Ethics concerning potential conflicts of interest or any legal impediments to your serving in this position?
Yes.

D. LEGAL MATTERS

1. Have you ever been disciplined or cited for a breach of ethics for unprofessional conduct by, or been the subject of a complaint to any court, administrative agency, professional association, disciplinary committee, or other professional group? If so, provide details.
No.

2. Have you ever been investigated, arrested, charged or convicted (including pleas of guilty or nolo contendere) by any federal, State, or other law enforcement authority for violation of any federal, State, county or municipal law, other than a minor traffic offense? If so, provide details.
No.

3. Have you or any business of which you are or were an officer, director or owner ever been involved as a party in interest in any administrative agency proceeding or civil litigation? If so, provide details.
No.

4. For responses to question 3, please identify and provide details for any proceedings or civil litigation that involve actions taken or omitted by you, or alleged to have been taken or omitted by you, while serving in your official capacity.
N/A

5. Please advise the Committee of any additional information, favorable or unfavorable, which you feel should be considered in connection with your nomination.
None.

E. FINANCIAL DATA

All information requested under this heading must be provided for yourself, your spouse, and your dependents. (This information will not be published in the record of the hearing on your nomination, but it will be retained in the Committee's files and will be available for public inspection).

AFFIDAVIT

Robert D. Jamison being duly sworn, hereby states that he/she has read and signed the foregoing Statement on Biographical and Financial Information and that the information provided therein is, to the best of his/her knowledge, current, accurate, and complete.

Robert D. Jamison

Subscribed and sworn before me this 1st day of October, 2009

Karen R. Williamson

Notary Public

Karen R. Williamson
Notary Public, District of Columbia
My Commission Expires 2/28/2011

U.S. Senate Committee on Homeland Security and Governmental Affairs
Pre-hearing Questionnaire
For the Nomination of Robert D. Jamison, to be
Under Secretary for the National Protection and Programs Directorate
at the Department of Homeland Security

I. Nomination Process and Conflicts of Interest

1. Why do you believe the President nominated you to serve as Under Secretary for the National Protection and Programs Directorate (NPPD)?

   I believe that the President nominated me for this position based on my past performance as Deputy Assistant Secretary for the Transportation Security Administration, as well as my understanding of the department and the challenges facing the National Protection and Programs Directorate. I also feel that my track record as Deputy Administrator for the Federal Transit Administration and Acting Administrator of the Federal Railroad Administration contributed to the decision to nominate.

2. Were any conditions, express or implied, attached to your nomination? If so, please explain.

   No.

3. What specific background and experience affirmatively qualifies you to be Under Secretary for the National Protection and Program Directorate?

   I have a broad range of management experience in the private, not-for-profit, and public sectors that I can bring to bear on the challenges facing the Directorate. I have a proven track record of success across diverse operating environments which positions me well to address the multi-faceted challenges across the varied mission areas of the 17 Infrastructure Protection Sectors, the cross cutting domains of cyber security and communications, as well as the challenges in the Directorate's other areas.

   My operational experience from United Parcel Service has given me a solid business acumen foundation and a focus on accountability, outcome-based performance metrics, and efficiency.

   On top of that business foundation, I have gained valuable operational management experience from the American Red Cross. The understanding of disaster relief operations complements my security experience and gives me a unique perspective into two critical areas involved in the important risk management and analysis work of the Directorate.

   At the Federal Transit Administration, I led process improvements to the oversight of large, complex, public transportation projects that resulted in improved schedule and

budget performance. My understanding and ability to instill strong project management, risk management, and good fiscal discipline into an organization will continue to benefit the Directorate as we face many large scale deployment projects.

Additionally, my tenure at the Federal Railroad Administration coupled with my regulatory responsibilities at Transportation Security Administration (TSA) gives me valuable experience to leverage as the Directorate rolls out the Chemical Facility Anti-Terrorism Standards and the continued development of the Office of Infrastructure Protection.

Finally, my tenure as the Deputy Assistant Secretary at TSA has given me tangible experience improving security across a complex and diverse operating spectrum. It also afforded me the opportunity to work closely with the private sector as well as our State and local partners to ensure collaboration and cooperation.

4. Have you made any commitments with respect to the policies and principles you will attempt to implement as Under Secretary for the National Protection and Programs Directorate? If so, what are they, and to whom were the commitments made?

   No.

5. If confirmed, are there any issues from which you may have to recuse or disqualify yourself because of a conflict of interest or the appearance of a conflict of interest? If so, please explain what procedures and/or criteria that you will use to carry out such a recusal or disqualification.

   No.

6. Have you ever been asked by an employer to leave a job or otherwise left a job on a non-voluntary basis? If so, please explain.

   No.

II. Background of the Nominee

7. What were your responsibilities while serving as the Deputy Assistant Secretary for the Transportation Security Administration (TSA)? What was the size of your staff?

   While Deputy Assistant Secretary I was responsible for all operating aspects of the 57,000 plus-person agency charged with the security of the Nation's transportation systems. I oversaw an average annual budget of 6.3 billion dollars.

8. What were your responsibilities while serving at the Department of Transportation (DOT)? What was the size of your staff?

While Deputy Administrator of FTA I was responsible for all operating aspects of the 520-person, ten-region agency that administered the Federal transit assistance program whose budget at the time was $7.6 billion. I directed the evaluation of the $1.5 billion New Starts program and oversight of all major Federal investments in public transit infrastructure. I played a lead role in the oversight of the funding to rebuild Lower Manhattan's transportation infrastructure after the terrorist attack and the development of FTA's security related programs.

While Acting Administrator of FRA I was responsible for all operating aspects of an 826-person, eight-region agency primarily responsible for the promulgation and enforcement of rail safety regulations. The budget of the agency was $1.4 billion which included funding for research and development and railroad assistance programs.

9. What were responsibilities while serving at the American Red Cross? What was the size of your staff?

I served in three different positions while at the American Red Cross of which two were the most prominent. I served in the role of Vice President of Chapter Operations where I was responsible for the development and management of health and safety products and services. The responsibilities included comprehensive portfolio management of the health and safety services that were delivered by 1296 (the number at the time) local Red Cross chapters. Chapter Operations had a $19 million corporate staff budget and 100 plus person staff.

The other role was Senior Operations Officer. In this role, I was the senior operations advisor to the Chief Operating Officer, who was responsible for all aspects of a $2.5 billion, 33,000-employee non-profit. I had direct input on and implementation of strategic planning, organizational alignment, infrastructure analysis, and management decisions. I was actively involved with all policy development, long-range planning, short and mid-term goal setting, and metrics development.

10. You served as the Deputy Administrator of the Federal Transit Administration during the response to Hurricane Katrina. What role, if any, did you play in the response, specifically in the execution of Emergency Support Function #1 (Transportation)?

Initially I played a limited role in the Katrina response other than ensuring FTA's minimal support role to DOT's crisis management center was effective. A few days after landfall, at the request of U.S. Department of Transportation Secretary Mineta, I led DOT's efforts (working with the Pipeline and Hazardous Materials Safety Administration) to restore service to the petroleum pipeline infrastructure. After we had worked with industry and our federal partners to substantially restore pipeline service, I was asked by Secretary Mineta to step into ESF#1 and play a lead role in the Katrina air evacuation efforts for DOT. Once the air evacuation was complete, I returned to my normal duties at FTA. As a part of my duties at FTA, I worked to help coordinate the restoration of public transportation infrastructure and the standup of temporary public transportation service to the affected areas.

11. Please provide the Committee with the written criteria which DOT uses in determining whom to award its War on Terrorism Medal as well as a copy of the citation awarding that medal to you.

Upon researching the award with DOT, I discovered that I received The War on Terrorism Ribbon and not the medal.

The War on Terrorism Ribbon recognizes contributions of employees who are not necessarily in positions of great responsibility, but whose performance has made significant contributions to the Nation's security while accomplishing the mission of the Department.

III. Role and Responsibilities of the Under Secretary for the National Protection and Programs Directorate

12. Why do you wish to serve as Under Secretary for the National Protection and Programs Directorate?

There are several reasons I wish to serve as Under Secretary for the National Protection and Programs Directorate, the primary being my desire to have an impact on what I consider to be some of the most important issues facing our Nation. The Directorate has an exciting and diverse mission with numerous challenges. I believe I can bring my skill set to bear on those challenges and improve the security of the Nation as a result.

13. What do you see as the principal mission(s) of the National Protection and Programs Directorate?

The Directorate has a diverse operating environment ranging from cyber security to the delivery of biometric identity services. However, there is an underlying principal mission that is common among all of the components of the National Protection and Programs Directorate. That common mission is risk reduction. The Directorate strives to make sound management decisions and to drive risk reduction across our areas of responsibility. The Directorate plays a fundamental role in improving the way risk is comprehensively measured and managed across the Department.

14. What do you see as the National Protection and Programs Directorate's strengths and weaknesses in its ability to accomplish those mission(s)?

The National Protection and Programs Directorate's core strength is the dedicated, loyal, and mission-focused staff. I mentioned earlier the Directorate's diverse operating environment. One of the benefits of that diverse operating environment is that NPPD has a talented workforce with different focused areas of expertise. Leveraging the strengths of the individual components to make the Directorate stronger as a whole would be one of my goals if confirmed.

Our greatest challenge is the fact that we are a new organization still in the process of transitioning into the organization that Congress and the Department have envisioned. We are in the formative stages of many of our programs and must be focused on attracting and retaining the talent and skills needed to mature these programs.

15. If confirmed, what would be your top priorities? What do you hope to have accomplished at the end of your tenure?

As I look at the challenges facing the Directorate, I would break down my priorities into two primary focus areas. If confirmed, I would strive to accomplish these priorities.

The first area of priority focus is the maturation of the Directorate. If confirmed, I would work hard to position the Directorate to grow and mature our risk reduction programs. My top priorities would be to a) attract and retain the skill sets needed to advance these programs and to successfully navigate the transition of administrations, b) foster improved teamwork across the Directorate and leverage the diverse skills across the individual components to make us better as a whole, and c) to improve fundamental business practices across the Directorate.

The Directorate has several major programs that are in key stages of development. If confirmed, my second priority focus area would be meeting key milestones in our most important programs. I would strive to successfully implement a) the Chemical Facility Anti-Terrorism Standards Regulations, b) US-VISIT's Air Exit regulation, and c) improved cyber security defense across the Federal government.

IV. Policy Questions

General Management

16. What is your approach to managing staff, and how has it developed in your previous management experiences?

My approach to managing staff is to first ensure I get right person in the right job. Once the right skill sets are developed or recruited into the right job, a leader must then give those staff strategic direction, ensure they are properly resourced, and prepare the way for their success by utilizing the position of leadership to break down barriers that could impede it. As my approach has matured over my years in management, I've found there is no substitute for having the right skills in the right job. I also strongly believe that successful leaders must give solid, high-level direction, but empower their staff to ensure they have the confidence to take the actions necessary to get the job done.

17. The Department of Homeland Security (DHS) may face a substantial challenge during the presidential transition in 2009 because of the high ratio of political appointees to federal employees employed at the Department. How do you intend to prepare the National Protection and Programs Directorate to successfully transition to a new Administration?

If confirmed, my top priority would be to get the right person in the right job. The execution of this priority includes ensuring we have the strong career leaders behind our political appointees. I will work closely with the Deputy Secretary and the Undersecretary for Management to ensure that we continue to make substantial improvements in this area as they address this issue across the Department. I would also continue efforts to carefully evaluate NPPD's utilization of contractor staff. I plan to effectively convert contract staff to Federal staff where appropriate to make the most efficient use of resources and to ensure we have the strong skills in government needed to position the Directorate for the future.

Personnel Management

18. What actions in your past executive experiences demonstrate your style and approach in the area of labor-management relations?

    My management experience in the not-for-profit, private, and government sectors has given me a unique view of labor-management relations across diverse operating environments. That experience has forged my management philosophy that the most important fundamental of good labor management relations is frequent, robust two-way communication. In my work at United Parcel Service and TSA, a key fundamental of improved relations was the development of empowered employee advisory councils. At my direction under my current NPPD role, the Directorate will soon be launching employee advisory councils.

19. The Department has been active in contracting out selected government functions. While contracting out can be an effective means of performing the department's activities, it is critical that the government have sufficient staff on board with the appropriate skills to establish policy, maintain a strong institutional memory, and to effectively manage acquisitions and contract oversight in order to ensure quality, economy, and timeliness. What are your views on the future of federal contracting and the capacity of the federal government to ensure that the public interest is appropriately served?

    The private sector brings a strong sense of mission, capability, innovation, and the ability to stand up to meet emerging requirements quickly and cost effectively. As a result, I understand why the Department has relied so heavily on contract support where appropriate.

    I do believe, however, that the appropriate mix of contractor and permanent Federal staff must be continually examined to achieve optimal balance between cost savings and operational continuity. In my current role, we are undergoing a careful evaluation of that balance in NPPD and are establishing conversion goals where appropriate to ensure we make the most efficient use of resources and to ensure we have the strong skills in government needed to position the Directorate for the future. If confirmed, I will strive to meet those targets.

20. The Office of Infrastructure Protection (OIP), in particular, relies heavily on contractors to fill many of its core missions. OIP reports using contractors for services ranging from administrative support and budget analysis to policy development and program oversight.

    a. What functions do you believe are appropriate only for permanent federal employees?

    Only permanent Federal employees should perform inherently governmental positions. While inherently governmental activities require the exercise of substantial discretion, this discretion must have the effect of committing the Government to a course of action when two or more alternative courses of action exist and decision making is not limited to the existing policies, procedures, directions, orders, or other guidance. At the Department, we have been particularly mindful of the need to limit contract involvement in adversarial actions or involvement in wide-ranging interpretations of complex, ambiguous case law and other legal authorities. We are also sensitive to actions that could significantly and directly affect the life, liberty, or property of individual members of the public, including the likelihood of the need to resort to force in support of a police or judicial function.

    That said, however, the private sector can bring a wealth of knowledge and resources to the table and can facilitate the gathering and the analysis of vast amounts of technical and programmatic data. Proper contract administration and good sense of oversight for the possibility of conflicts-of-interest that may exist from any service provider are always necessary.

    b. What is the ratio of contractors to federal employees in OIP (measured either in hours worked or budget expended)?

    In FY07, there were 302 full time employees and 292 contractors in OIP.

    c. Do you believe OIP should transition towards using less contractors and more permanent federal employees? Why or why not?

    I believe we need to be careful in our examination of options so that we have both the resources necessary and the appropriate balance between contractors and permanent Federal employees in OIP. In my current position, I have asked my budget and human capital staff to bring me recommendations on where we might need to rebalance the mix so that I may act appropriately on their findings.

Critical Infrastructure Protection

21. OIP is responsible for coordinating national efforts to reduce risk to our critical infrastructures and key resources (CI/KR) posed by acts of terrorism. OIP is to facilitate the identification, prioritization, coordination, and protection of CI/KR in support of Federal, State, local, territorial, and tribal governments, as well as the private sector and international entities.

a. What is your assessment of the key challenges facing our country with respect to protecting critical infrastructure?

Protecting and ensuring the continuity of the critical infrastructure and key resources (CI/KR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. CI/KR include the assets, systems, networks, and functions that provide vital services to the Nation. Terrorist attacks on CI/KR and other manmade or natural disasters could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the affected CI/KR and physical location of the incident.

Improving the protection of the Nation's CI/KR in an all-hazards environment requires a comprehensive, unifying organization; clearly defined roles and responsibilities; and close cooperation across all levels of government and the private sector. Protection authorities, requirements, resources, capacities, and risk landscapes vary widely across governmental jurisdictions, sectors, and individual industries and enterprises.

The enormity and complexity of the Nation's CI/KR, the distributed character of its associated protective architecture, and the evolving and uncertain nature of the terrorist threat and manmade or natural disasters are the key challenges.

b. What challenges do you see facing OIP in implementing its mission?

OIP faces the challenge of ramping up capabilities to address the new authorities such as executing the Chemical Facility Anti-Terrorism Standards Regulations. Additionally, OIP must continue to mature the National Infrastructure Protection Plan (NIPP) and supporting Sector Specific Plans (SSP) process. OIP must continue to foster its private sector partnerships while proactively ensuring that the risk reduction measures are implemented and that OIP programs are resulting in measurable progress.

22. How important do you believe it is that critical infrastructure policy focus on continuity of operations and contingency plans so that critical assets can be quickly reconstituted after a catastrophe?

Incorporating critical infrastructure policy into the continuity (COOP/Contingency) programs and plans is not only essential, it is now required by the National Continuity Policy Implementation Plan signed by President Bush in August 2007. With the appropriate contingency plans already in place, a starting point for incident mediation or recovery is readily available immediately following an incident. Without the appropriate plans and COOP measures in place, reconstitution of CI/KR could require a significant diversion of existing resources, often taking experts with other critical roles days to develop a tailored incident-specific plan.

23. How do you respond to concerns that the private sector, which owns 85% of our nation's critical infrastructure, may lack sufficient incentive to invest in securing key assets, particularly if their competitors are not held accountable for meeting the same standards?

Leading companies not only recognize that good risk management offers benefits against other manmade and natural hazards, they also work with us to implement the most current best practices. The more the Department can communicate success stories, share effective security practices, and offer timely and focused information back to the private sector, the greater the incentives to invest in security will be. In addition, OIP must continue to improve its measurement of those security activities in the field to ensure that our critical infrastructure is protected.

24. In June 2006, DHS issued the National Infrastructure Protection Plan (NIPP) to provide a unifying structure for the integration of critical infrastructure and key resources protection into a single national program and to define critical infrastructure roles and responsibilities for all levels of government, private industry, nongovernmental agencies, and tribal partners.

    a. What do you see as your priorities in the implementation of the NIPP and what specific milestones do you believe need to be achieved over the next year?

    Some of the most important priorities for the coming year include improving information sharing through Homeland Security Information Network (HSIN), completion of CI/KR protection program gap analyses, improving information protection of key C/KR, and continued private sector participation.

    b. The NIPP relies on voluntary cooperation from industry. Each sector has submitted a Sector Specific Plan (SSP), as required in the NIPP, but it's unclear to what extent the SSPs are considered a useful tool by the sectors and whether they'll be implemented effectively. Do you believe the NIPP lays out a policy that sufficiently compels private sector participation in critical infrastructure protection?

    Effective implementation of the NIPP is predicated on the active participation by government and private sector security partners and the establishment of a mutually beneficial, trusted relationship. Except in limited instances, the private sector's participation and compliance is voluntary, and the Department is proactively working to establish programs and processes that ensure the continuance of these government-private sector partnerships.

    One of the programs OIP has established is the national and sector-specific CI/KR measurement and analysis (metrics) process. OIP collects information on the usefulness of the SSPs as a planning tool. Information collected from the sectors indicates that the NIPP partnership framework has had a positive impact on information sharing and coordination. Most sectors are actively seeking new members for sector Government Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs), and some sectors have even established formal cross-sector coordination. As the process matures, I believe that OIP needs to ensure that the metrics continue to mature and become more outcome-focused.

c. How do the NIPP and 17 SSPs relate to the numerous field activities, grant programs, and other departments and agencies' actions to harden our Nation's CI/KR?

The NIPP and SSPs provide a structure wherein exercises and training, grant awards, and allocations can be based on risk, rather than perception, fear, or the most recent incident that has been experienced. Over the next few years, these programs and efforts will become more coordinated and linked, which will maximize the benefits of our critical infrastructure protection expenditures by focusing on the greatest risks, minimizing redundant efforts, and identifying critical gaps.

25. The NIPP states that since it is not possible to protect all assets against every possible terrorist attack, a risk based approach "driven by intelligence analysis and reporting" is critical to an effective risk mitigation strategy and efficient resource allocation.

a. Do you believe that current quality of intelligence analysis and reporting is at the level necessary to effectively implement the NIPP?

Good intelligence is the most effective security measure that we have. The establishment of the Homeland Infrastructure Threat and Risk Assessment Center (HITRAC), a joint program office that performs integrated threat and risk analysis for U.S. critical infrastructure and key resources by bringing together intelligence and infrastructure analysts from both organizations, has improved our ability to collect and disseminate key information. HITRAC has been successful in providing information to State, local, tribal and private sector partners on the nature of the threat they face and how the unique vulnerabilities of the Nation's infrastructure can be exploited to support their strategic security planning as outlined in the NIPP. However, we must continue to strive to improve our efforts in this area.

b. Are efforts within NPPD to develop risk modeling and final CI/KR risk assessments duplicated in other parts of DHS?

Risk modeling analysis is occurring in various components throughout the Department for their specific requirements. With the establishment of the Office of Risk Management and Analysis (RMA), we are working to develop a risk methodology that leverages risk products to inform a consolidate risk approach for the Department as a whole.

c. How does DHS's Office of Intelligence and Analysis, NPPD's Office of Risk Management and Analysis, OIP's Homeland Infrastructure Threat & Risk Analysis Center (HITRAC), and the national laboratories coordinate efforts to produce the Tier I/Tier II CI/KR lists?

The development of Tier 1/Tier 2 CI/KR lists is an annual effort led by HITRAC. Federal, state and local, private sector, and other security partners provide asset and system information and analysis as inputs to the Tier 1/Tier 2 program. Specifically, the Office of Intelligence and Analysis provides threat assessments that describe

terrorist interest in specific assets or facilities, which are included, at a minimum, on the Tier 2 list. The National labs, NISAC in particular, provide in-depth consequence and interdependency analysis for the National assets and systems of most concern.

d. How do other departments and agencies, states and local communities, tribal entities, and the private sector add to this process?

All of NPPD's critical infrastructure analysis efforts are collaboratively developed with security partners throughout the infrastructure protection community from the Federal and State governments down to the private sector. All of these groups have official representation through the NIPP partnership model on groups such as Government and Sector Coordinating Councils, the Partnership for Critical Infrastructure Security and the State, Local, Tribal, Territorial Government Coordinating Councils. These groups, along with ongoing informal relationships between NPPD and its partners, provide the information and expertise that enhances all of NPPD's analyses.

26. In a July 2007 hearing held by the Subcommittee on State, Local, and Private Sector Preparedness and Integration titled "Private Sector Preparedness, Part II: Protecting Our Critical Infrastructure," a witness from the Government Accountability Office (GAO) referred to the SSPs as "plans to plan." GAO also reported that the comprehensiveness of the SSPs varied by sector stating, "it is unclear the extent to which DHS will be able to use them to identify security gaps and critical interdependencies across the sectors."

a. What do you believe is the value and purpose of the SSPs?

The greatest value of the SSPs is that they serve as the unifying vehicles across one or more sectors. They provide a common way for diverse parts of one sector to discuss infrastructure protection, determine requirements and priorities, and start to address those priorities. The SSPs allow those who know the unique issues of the sector to reflect and address those concerns in a comprehensive and consistent manner.

b. What do you see as the next steps in implementing the SSPs?

I believe that tremendous progress has been made in the development of the SSPs. However, I agree that the comprehensiveness of the plans varies by sector and that OIP must continue drive the development of more mature plans. The next steps in SSP implementation are to take the actions needed to ensure an effective, efficient program over the long term. Our goal is to raise the security baseline in each sector by maturing the plans and ensuring their execution by using outcome-based metrics.

27. The DHS strategy for protecting critical infrastructure includes efforts to foster the sharing of information by infrastructure owners about security vulnerabilities and incidents.

a. How important do you believe such information sharing is, and how successful do you believe current government policies and efforts have been at achieving such information sharing?

Very important. The sharing of information between the Federal Government, State/Locals and Owner/Operators of CI/KR is one of the primary drivers for the overall protection of CI/KR. Information that is relevant and actionable informs Owners/Operators of CI/KR and enables decision making in three different areas: 1) strategic planning and investments in security, 2) situational awareness and preparedness to respond to and mitigate consequence, and 3) operational planning and response.

I believe that the NIPP process has spurred dramatic improvements in information sharing and that we need to continue to build upon that improvement. The formation of the NIPP Sector Partnership has been a significant step and a foundation for the effort to develop the trusted environment that encourages appropriate information sharing. In addition, the implementation of the final rule of the Protected Critical Infrastructure Information (PCII) Program adds to the building of such a "trusted" environment by mitigating the risks that come with public-private information sharing. Substantial work has been performed to encourage and remove barriers to the owners and operators of the critical infrastructures to participating in an information sharing environment. In addition, to the Sector Partnership and the PCII Program, the NIPP describes other information sharing mechanisms and tools that provide the structure and processes, ranging from electronic platforms to operations centers that act as hubs for private sector coordination, on which public and private sector security partners exchange vital information in order to mitigate the Nation's critical infrastructure risks. We must continue to improve information sharing.

b. What, if anything, do you believe should be done to improve the sharing of security related information by the owners of critical infrastructure?

I believe we need to continue to build on our partnership model. Through the Sector Partnership, the Department continues to work with the Critical Infrastructure/Key Resource Sectors (CI/KR) to develop mutually agreed upon processes, requirements, and structure to implement a "trusted" information sharing environment. The private sector continues to fear the liabilities that they incur when sharing information with public entities, and the potential losses that come with exposure of proprietary information. DHS must ensure that the value of the information to the owners and operators must exceed the information sharing risks to encourage and sustain an appropriate exchange. DHS must continue to work with the Sector Partnership, as described in the NIPP, as it continues to mature and grow in stature, on the quality, timeliness, and usefulness of the information exchange.

c. Do you believe DHS has redundant or similar share information sharing programs, and if so what is the impact of such duplication?

The Department was created out of 22 different agencies. Many different programs, including information sharing, came together under the DHS umbrella as a result. Many represent longstanding and successful legacy activities that came under a common the Department mission—to protect the Homeland. Sharing information among each other and with their partners is imperative to each component, as well as for the Department's success. I believe that many of the actions that the Department has taken over the last year are improving the process, but that more work must be done. Over the last year, the Department has implemented an Information Sharing Governance Board and an Information Sharing Coordinating Council (ISCC) to improve coordination of information sharing among the components of DHS. These coordination efforts will streamline and codify information sharing processes across the Department.

28. While OIP is responsible for the overall protection of critical infrastructure, other component agencies within DHS have regulatory authority for security matters over specific sectors. For instance, TSA's mission is to protect the Nation's various transportation systems.

    a. What role do you see OIP having in the protection of critical infrastructure sectors which are regulated by other component agencies within DHS, including TSA or the Coast Guard?

    OIP continues in its role to lead the coordinated national effort to protect CI/KR. Outside of TSA and the Coast Guard, there are a number of preexisting and, in the case of the Chemical Facility Anti-Terrorism Standards, new authorities in place in agencies and departments such as the Nuclear Regulatory Commission (NRC) and the Department of Transportation that affect CI/KR assets. OIP works with the SSAs to ensure that all NIPP-related implementation activities, which may include a regulatory program, are in progress and that reporting requirements are met. The NIPP defines roles and responsibilities for Sector Specific Agencies (SSAs), such as TSA and the Coast Guard, recognizing that each CI/KR sector possesses its own unique characteristics, operating models, and risk landscape.

    b. In these cases, do you believe OIP should play a supportive role, direct such agencies to carry out policies and practices developed by OIP, coordinate the efforts among the myriad offices or agencies with some responsibility for different critical infrastructure sectors, or should fill some other role?

    Yes, in order to mandate compliance with particular requirements, the Department would need additional statutory authority. The Department leads the coordinated national effort to reduce risk to our critical infrastructures and key resources (CI/KR) posed by acts of terrorism, and enables national preparedness, timely response and rapid recovery in the event of an attack, natural disaster, or other emergency. DHS both supports and coordinates with other Federal agencies including all of the SSAs and a host of other partners. OIP is the Department's lead for ensuring the identification, prioritization, coordination, and protection of CI/KR in support of Federal, State, local, territorial, and tribal governments, as well as the private sector,

and for providing information sharing mechanisms about threats, vulnerabilities, incidents, potential protective measures, and best practices that enhance protection, response, mitigation, and restoration activities.

29. The majority of critical infrastructure sectors are not subject to federal security regulation.

    a. In your opinion, are there any sectors that are not currently regulated and should be? If so, which ones and why?

    Most of the CI/KR sectors, outside of the transportation and chemical security sectors, are not subject to Federal security regulations. As such, I believe the Department would need additional statutory authority to mandate compliance with particular requirements. The Department is committed to continuing to support the numerous voluntary security programs in place in and among the sectors as set forth in the Sector Specific Plans under the NIPP. OIP must continue to work with all partners to determine, based on the evolving threat and risk landscape and the current security measures in place, if any sector may need additional protection. We will also use the results of the CI/KR NAR process to inform this dialogue as well. As DHS has demonstrated in the past, NPPD will aggressively pursue additional regulatory authority and regulations if needed to ensure the Nation's critical infrastructure is protected.

    b. Do you believe new authority from Congress would be required for the Department to regulate additional sectors?

    As noted above, I believe additional statutory authority would be necessary to mandate compliance with particular requirements. OIP will continue to work with all partners to identify, in the evolving threat and risk landscape, any sector that may need additional protection. We will also use the results of the CI/KR National Annual Report collaborative process to inform this dialogue as well.

Chemical Security

30. As the Department's chemical site security program gets underway, it is important that the Department have the appropriate resources and expertise to assess the facility plans and ensure compliance.

    a. Please discuss the current budget requirements for this program, including projected increases and whether current available funding is sufficient to keep the program on schedule.

    The President's budget request for fiscal year 2008 of $25 million currently appears sufficient to ensure meaningful implementation for the first phase of the CFATS program. Since we continue to learn much about the landscape of the sector as we implement the regulations, we are closely monitoring changing funding requirements.

b. The program is progressing in stages, addressing the most critical facilities first. It appears that additional funding would enable the Department to implement requirements at a larger number of facilities more quickly than currently planned. Is this correct or are there other impediments to expanding the program to all of the facilities that will eventually be covered?

The Department has prioritized the most critical facilities based on current information, and these requirements are reflected in the President's budget request for fiscal year 2008. We will continue to monitor changing funding requirements as we gain more information during the initial phase of CFATS implementation.

c. Please describe the role of contractors in designing and implementing the chemical site security program, as well as planned additions to permanent Department staff.

The chemical security compliance program does employ a small number of contractors who have contributed to implementation of the CFATS program by providing subject matter expertise in the areas of chemical process safety, physical security, chemical engineering, computer-coding and algorithm development, and other technical areas.

Based on detailed resource and staffing analysis, in FY 2007 the Department is hiring 33 new full-time Federal staff for the chemical security program, and an additional 30 full-time Federal staff in FY 2008.

d. Please describe any plan to transition temporary Federal Protective Service inspectors to permanent OIP FTEs.

As part of a departmental effort to transition contractors to FTEs where appropriate, the chemical security compliance program plans on transitioning from detailed Federal Protective Service (FPS) inspectors to permanent OIP inspectors beginning in FY 2008. The first planned step is to transition to an OIP inspector management cadre. The second step is to transition from detailed FPS inspectors to an actual inspector cadre of OIP FTEs. Both steps will be accomplished using currently available hiring tools. The transition of qualified FPS detailees to OIP permanent inspector positions by their applying for positions via the hiring process would be welcomed and provide greater continuity, but their transition in not required for continued program long-term success.

31. Given the new Chemical Facility Anti-Terrorism Standards (CFATS) regulatory approach intended to focus efforts on specific sites "high-risk" sites rather than impose regulations cross the entire sector, what efforts are being made to ensure any list of these sites is consistent with other DHS "risk or tiered lists?"

Under CFATS, the Secretary may determine at any time that a chemical facility presents a high level of security risk based on any information available – including information

submitted under CFATS such as the Top Screen or Security Vulnerability Assessment (SVA) – that, at the Secretary's discretion, indicates the potential that a terrorist attack involving the facility could result in significant adverse consequences for human life or health. High-risk facilities are assigned to one of four tiers based on risk.

Outside of CFATS, the Department also manages and coordinates voluntary security programs with the private sector and State and local entities. Data collected through open sources, intelligence, or information voluntarily submitted to the Department is used to identify risks and prioritize critical assets. These "risk or tiered lists" are eligible to participate in DHS security programs, including grants available to State, tribal, and local government. Through internal Departmental coordination, high-risk chemical facilities as defined by CFATS are part of these broader voluntary Departmental efforts and information is reviewed and acted upon on a case-by-case basis, ensuring that voluntary programs and compliance requirements under CFATS are complementary.

Office of Bombing Prevention

32. The Office of Bombing Prevention (OBP), located within OIP, is charged with coordinating federal bombing prevention efforts. In FY 05 and FY 06, OBP was funded at $14 million. In FY 07, OBP's funding decreased to $5.17 million, and in FY 08, the President requested $6.14 million. Given the increasing threat of improvised explosive devices (IED), do you believe OBP can successfully execute its mission with this decreased level of funding?

    The Department and the OBP continue to prioritize the mitigation of the threat posed by IEDs. The Department has invested in IED detection across the Department, for example over a billion dollars in TSA on detection, additional canine teams and checkpoint technology; $70 million dollars has been invested in research and technology in Science and Technology; $200 million for radiological and nuclear detection equipment for DNDO; and $340 million for inspection detection technology for Customs and Border Protection; $200 million for port security grants; and $175 million for rail and transit security grants.

33. On September 10, 2007, Secretary Chertoff testified that the Department will soon deliver to Congress a strategic document detailing what is being done to counter improvised explosive devices (IEDs).

    a. When will that plan be delivered?

    The HSPD-19 is being led by the Department of Justice and the Report is currently pending interagency clearance and then Presidential approval. The Department believes the Report will be approved and delivered in the very near future. As the Secretary has stated, the Department has already begun implementing many of the recommendations in the HSPD-19 Report.

b. The Department was required by law to deliver a National Strategy for Bombing Prevention to Congress by January 2007. This document has not been received. Will you please explain why the Strategy has not been delivered?

DHS completed the substance of the National Strategy for IEDs (NSIED) in January, 2007 and aggressively began implementation of key recommendations during the development process itself. The development of the National strategy focused interagency attention on the IED issue, and influenced the President's decision to release Homeland Security Presidential Directive 19 (HSPD-19). HSPD-19 requirements superseded the NSIED in scope and authority, directing the Department of Justice (DOJ), in coordination with the Department of Homeland Security and the Federal interagency, to build upon the strategic concepts and objectives articulated in the congressionally mandated effort and develop a strategy and recommendations. The HSPD-19 Report is currently pending interagency clearance and then presidential approval, and will be delivered to Congress as soon as it is approved by the President.

c. Is the strategic plan referenced in Secretary Chertoff's testimony meant to fulfill that congressional mandate?

Yes. The strategic document referred to in Secretary Chertoff's testimony is the HSPD-19 Report. The HSPD-19 Report is currently pending interagency clearance and then Presidential approval, and will be delivered to Congress as soon as it is approved by the President. The delivery of the HSPD-19 Report will fulfill the Congressional mandate for a "National strategy for bombing prevention."

Protective Security Advisors

34. To assist state and local governments and the private sector with critical infrastructure protection, OIP places Protective Security Advisors (PSAs) throughout the country.

a. How does OIP ensure that the PSAs are coordinated with other local DHS representatives present in the same community, such as the FEMA regional offices?

PSAs interact and coordinate with a large number of individuals and organizations at all levels of government and within the private sector. As the DHS critical infrastructure protection representatives in the field, PSAs regularly interact with State Homeland Security Advisors, Emergency Management Directors, and other Federal, State, territorial, local, tribal and private sector security partners. Examples of this interaction include:

- *PSA Minneapolis, MN provided situational awareness and support State and local officials after the I-35W bridge collapse on 1 August 2007.*
- *Supervisory PSAs Gulf Coast Area, Southeast Area, and Southwest Area, and PSAs Little Rock, AR, Tampa, FL, Baton Rouge, LA, Oklahoma City, OK, Austin,*

TX, Dallas, TX, and San Antonio, TX provided situational awareness and support to State and local officials during Hurricane Dean from 18-22 August 2007.

- *PSAs Jackson, MS provided situational awareness and support to State and local officials during the Chevron Refinery fire on 16 August 2007.*
- *PSAs participate with the United States Coast Guard in Area Maritime Security Committees.*
- *PSAs coordinate with United States Customs and Border Protection regarding international bridge crossings listed as high-priority CI/KR.*
- *PSAs, often co-located with the United States Secret Service, coordinate with that agency during special events such as the Super Bowl and the United Nations General Assembly.*

In addition, PSAs in the field also interact and coordinate with FEMA Federal Coordinating Officers (FCOs) and Regional Administrators as necessary; liaison with Regional Response Coordination Centers (RRCC); and provide support to Joint Field Offices (JFOs) as necessary during incidents.

b. How does the PSA program support not only the NIPP, but other field activities?

PSAs serve as DHS' on-site critical infrastructure and vulnerability assessment specialists. They provide a vital channel of communication between the Department and State, local and tribal officials and private sector owners and operators. In addition, PSAs provide support to officials responsible for special events planning and exercises; and provide real-time information on CI/KR, as well as protective measures, often providing support to State and local representatives in State and local Emergency Operations Centers (EOCs).

Because they are located throughout the United States, PSAs are often the first DHS personnel to respond to incidents. Consequently, PSAs are uniquely able to provide early situational awareness to the Department's leadership during an incident, often performing duties as the Infrastructure Liaison (IL) in support of the Principal Federal Official (PFO) and/or the Federal Coordinating Official (FCO). PSAs also coordinate requests from CI/KR asset owners and operators for services and resources to include Surveillance Detection and Soft Target Awareness training, scheduling of Site Assistance Visits (SAVs), Buffer Zone Plans (BZPs), Comprehensive Reviews (CRs), and verification and technical assistance visits.

c. There are currently 78 PSAs nationally. Some large states have multiple PSAs and in some areas one PSA covers multiple states. There are currently 10 states sharing a PSA with a neighboring state. Please explain how OIP allocates PSAs across the country.

The FY 2005 House Report 108-541, accompanying the FY 2005 Department of Homeland Security Appropriations Act (PL 108-334) provided funding for 56 PSA positions. Locations for these positions were aligned with the then 56 FBI Joint

Terrorism Task Force (JTTF) locations. In addition, the Appropriations Committee provided funding for 12 additional PSA positions, directing that "they be allocated in such a way as to ensure that those areas with greater concentrations of critical infrastructure have adequate coverage, even if this requires assigning more than one PSA to a given location." In FY 2006, one PSA position was added at PSA Program headquarters, and nine Supervisory PSAs were added to the Program to optimize the efficient management of the PSA Program and meet the intent of the Congress in directing the placement of positions in the field, bringing the total number of PSAs to 78.

Public Information

35. The Critical Infrastructure Information Act (CIIA), enacted as part of the Homeland Security Act, was intended to establish a framework within which infrastructure owners would provide information about security vulnerabilities and incidents to DHS, and under which DHS would use that information in working to respond to incidents and to reduce vulnerabilities.

    a. Do you believe the CIIA has been effective at furthering the purposes for which it was enacted?

    Based on the PCII Program's accomplishments to date, I believe the CIIA has effectively furthered the purposes for which it was enacted, namely to facilitate the flow of Protected Critical Infrastructure Information (PCII) from private sector entities and State and local government entities to all levels of government. The PCII Program Office located within the National Protection and Programs Directorate of the Department is tasked with implementing the CIIA as directed in the Regulation at 6 CFR Part 29. To date, the PCII Program Office has accredited 2 Federal government entities external to the Department and 6 State and local entities to access PCII. Another 48 Federal, State and local entities are in the process of becoming accredited, and their accreditation is contingent on their meeting the accreditation requirements. In addition, the PCII Program Office has trained 1,323 users at the Federal, State and local government levels to access PCII. Finally, the PCII Program has partnered in a number of the Department and Federal agency information sharing initiatives[1] to integrate CIIA protections into those initiatives to foster greater information sharing.

    b. What, if anything, do you believe should be done to make the CIIA more effective?

[1] DHS initiatives include the National Cyber Security Division's United States Computer Emergency Readiness Team (US-CERT) Secure Portal Submissions Capability, the Infrastructure Information Collection Division's Risk Analysis and Management for Critical Asset Protection (RAMCAP) Program and Constellation/Automated Critical Asset Management System (ACAMS), and the Protective Security Coordination Division's Chemical Comprehensive Review, Site Assistance Visits (SAVs) and Buffer Zone Plans (BZPs).

To further the CIIA's mandate, DHS should continue to identify and refine its critical infrastructure information requirements such that potential submitters and information sharing partners are familiar with them and their integration of PCII.

c. How has the private sector responded to the Protected Critical Infrastructure Information (PCII) Program, which was established under the CIIA? How have state and local agencies, and how have community organizations that seek access to information, responded?

Stakeholders, both in the private and public sectors, have responded positively to the PCII Program. PCII submissions, requests for accreditation and information sharing partnerships continue to increase.

The number of information sharing partnerships within DHS that use PCII protections (see footnote 1) and those external to DHS, such as other Federal agencies, State and local entities to include Fusion Centers, speaks to the enthusiasm with which the Program is being embraced.

d. What additional actions, if any, are needed to improve this program?

DHS' *continued focus on defining its information requirements, dissemination methods and how the information will be used contributes substantially to the successful accomplishment of the PCII Program's mission. The more specific DHS can be with regard to its critical infrastructure information needs, the better the PCII Program is able to define its information protection role.*

36. Some have argued that the CIIA establishes a broader exemption from the Freedom of Information Act (FOIA) and other sunshine laws than necessary, and that the accountability of government and infrastructure owners suffer as a result. Others have argued that, notwithstanding the CIIA, infrastructure owners will not share necessary security related information unless the government mandates them to do so.

a. What is your opinion of those arguments?

I believe that the CIIA and the implementing Regulation, as well as policies, procedures and practices established by the PCII Program, are such that they do not establish a broader exemption from FOIA and sunshine laws than is necessary. In particular, the PCII Program has a validation process to determine whether submitted information (a) meets the definition of CII as set forth in the CIIA, (b) is not customarily in the public domain at the time it is validated and (c) has been properly submitted by the owner of the information or the owner's authorized representative. These safeguards ensure that appropriate information receives PCII protection. In addition, because the use of PCII is constrained (i.e. can only be used for homeland security purposes), the universe of information that can be validated as PCII is further limited.

CI/KR asset owners are justifiably concerned about the security of their sensitive information, but the protections provided by the CIIA and implementing regulation have done a great deal to encourage voluntary information sharing. In addition to the many government-initiated partnerships using the PCII Program to encourage and support information sharing, major corporations and large and small asset owners have acted to establish relationships to provide and protect CII.

b. What, if anything, do you believe should be done to improve government policy for getting infrastructure owners to share the information related to critical infrastructure security?

Based on the operational experience of the PCII Program, infrastructure owners are more likely to share their critical infrastructure information with the government if they get some sort of benefit from the program (such as, for example, a vulnerability analysis of their critical infrastructure compiled by local law enforcement in coordination with DHS).

Office of Cyber Security and Communications

37. What are your plans for completing a strategic plan that includes mechanisms to evaluate the performance of the entities under the Office of Cyber Security and Communications which includes the National Communications System, National Cyber Security Division, and Office of Emergency Communications?

With the standup of the Office of Emergency Communications (OEC) on April 1, 2007 and the formal grouping of the NCS, NCSD and OEC within a single Office of Cyber Security and Communications (CS&C), the Department initiated a series of strategic planning initiatives to ensure a common, focused vision for these three closely-related entities. These will more clearly define progress in our key missions.

38. Do you believe that DHS should merge IT and telecommunications critical infrastructure protection responsibilities for the National Communications System and the National Cyber Security Division?

In effect, these responsibilities were merged with the creation of the Office of Cyber Security and Communications (CS&C). The creation of CS&C is recognition by the Department that the technological convergence between IT and communication sectors is taking place. It is a clear sign that the Department is working closely with both IT and communications sectors to coordinate efforts. More importantly, the creation of CS&C acknowledges the importance of the increased cooperation and information sharing that is required between these two sectors as they evolve; government can evolve with them.

39. In June 2006, DHS concurred with GAO's recommendation that the Department review the National Communications System and National Cyber Security Division organizational structures and roles to address the convergence of the voice and data communications. On October 1, 2007, Assistant Secretary Greg Garcia stated: "With the

convergence of the IT and communications sectors, we need to ensure synchronized information sharing and response capabilities across our communications and cyber networks, precisely because those networks are becoming one and the same."

a. What is DHS doing to ensure that this information sharing across networks is occurring?

DHS, through the Office of Cyber Security and Communications (CS&C), is ensuring that operational activities involving information technology (IT) and communications networks are coordinated, threats and vulnerabilities are jointly addressed, and the resources and expertise of each organization are brought to bear in this converged environment. CS&C is implementing a plan to collocate the United States Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center for Telecommunications (NCC) watch and operations centers to ensure that IT and communications experts work side-by-side to: 1) share situational awareness, 2), identify and analyze vulnerabilities and attack vectors, 3) analyze implications across all infrastructure sectors, and 4) develop mitigation strategies.

b. If confirmed, how will you reorganize DHS components to deal with the convergence of voice and data communications?

The Department recognizes the significance of the convergence of IT and communications. The Office of Cyber Security and Communications (CS&C) brings together the National Cyber Security Division (NCSD) and the National Communications System (NCS). The responsibilities of NCS and NCSD are complementary, and reflect both the distinctions between and the convergence of the IT and Communications Sectors.

NCS and NCSD collaborate on a regular basis on a variety of issues, including infrastructure protection, research and development requirements, operational response activities, standards and best practices, international partnerships, in addition to collaboration, exercises, and other strategic initiatives.

40. In order to establish strong leadership within the Department for issues related to interoperable communications, Congress established the Office of Emergency Communications (OEC) when it passed the "Post-Katrina Emergency Management Reform Act of 2006" (P.L. 109-295) (Post-Katrina Act). OEC unites functions related to interoperability that previously were dispersed throughout the Department. Under 6 U.S.C. 1801(f), as established by the Post Katrina Act, the Secretary of Homeland Security was to submit to Congress, no later than 120 days after the date of enactment, a report on the resources and staff necessary to carry out the responsibilities of the Office of Emergency Communications. The Department has not transmitted this report to Congress. What are your plans for ensuring that this overdue report is completed so that Congress may more accurately assess the budget and staff needs of OEC?

Emergency Communications is a priority for the Department of Homeland Security and the National Protection and Programs Directorate. The newly formed Office of Emergency Communications (OEC) is working diligently to complete this report as expeditiously as possible. The process for building the OEC and drafting this document was thoughtful and measured. A steering committee of senior leaders from throughout the Department was brought together to guide both efforts.

Our efforts to develop a complete picture of the needs, roles and responsibilities of this new Office were extremely complex and time consuming. Entities from throughout the Department, including the Directorate for Science and Technology, the Directorate for Management and the Federal Emergency Management Agency, have devoted significant time and energy to ensuring that the Sufficiency of Resources Plan is as accurate and detailed as possible. The Sufficiency of Resources Plan is currently in the final approval stages and I am personally engaged in this process.

41. In its recent assessment of DHS's progress over the last 4 years, GAO concluded that DHS had generally not achieved 5 of 6 interoperable communications performance expectations related to implementing the program, procedures, standards, performance metrics and guidance, and technical assistance to first responders. How would you assess the status of the program and what are the three most important actions the agency should take to ensure the success of the program?

The creation of the Office of Emergency Communications was an important step towards addressing this challenge. The combination of the SAFECOM and the Interoperable Communications Technical Assistance Program (ICTAP) programs has been a force multiplier for the Department.

The Department must ensure all Interoperable and Operable communications efforts across the Department, including grant funding, are targeted at complying with the National Emergency Communications Plan (NECP). The NECP will establish the first National framework for establishing priorities, goals, milestones, and recommendations for advancing interoperable and operable emergency communication; it will serve as a partnership model that fosters relationships and facilitates coordination among Federal, State, regional, local, and tribal governments, and between emergency response and private sector partners.

We continue to engage regularly with State and local Emergency Responders. It is these individuals and agencies who are truly the first line of defense in the vast majority of incidents. By understanding the needs and requirements of these responders, the Federal government can work in partnership to advance the cause of Homeland Security throughout the Nation. There are currently a number of venues where Federal, State, local and tribal representatives meet to discuss interoperable and operable Communications, including the SAFECOM Executive Committee and Emergency Response Council and numerous National associations, such as the National Public Safety Telecommunications Council.

42. Along with its cyber responsibilities, the Office of Cyber Security and Telecommunications was established to address the preparedness communications needs for Federal, State, local, and private governments as well as private industry. Responding to communications needs has been a troubled area ever since the September 11 attacks.

    a. What specifically would you do to make rapid strides in meeting critical communication security needs?

    If confirmed, I intend to make improvements in the methodology of measuring the effectiveness of emergency and preparedness communications in the field. Establishment of more effective outcome measures will inform our program delivery and focus our resources on the most prevalent and highest risk issues. Good measurement will also allow us to better utilize our grant programs to drive continual improvement.

    b. How well do you believe DHS has addressed this problem?

    Working with industry and other Federal Agencies, such as the FCC, DHS has implemented a set of risk mitigation programs that collectively provide a high level of security and assurance for our Nation's communication systems.

    NCS has held annual training events for those personnel that would respond to a disaster upon activation. These training events, held recently in Homestead, Florida, and New Orleans, Louisiana, include participants from the Departments of Defense, Interior, Commerce, Homeland Security; local first responders; State public utility commissions; and many others. As a result of these events, the Department has identified and trained personnel to equip three Emergency Communications Teams prepared to respond.

    The National Communications System has been working to encourage the use of the "Next Generation Networks" which provide priority wire line service. Currently we have over 170,000 National security and emergency preparedness users, including approximately 19,000 State government users and 32,000 local government users.

    Additionally, NCS is planning to deploy a satellite communications service. This service will be a backup satellite service for voice communications serving critical Continuity of Operations/Emergency Operations Centers. This satellite service will minimize the reliance on the public communications network during times of disaster.

43. Do you believe any changes are needed in the current organizational and management structure of DHS to better address cyber security?

    As you know, the Department has made a number of changes to better address cyber security in the past several months, including the naming of an Assistant Secretary for Cyber Security and Communications and adding the Office of Emergency Communications to his responsibilities. We are striving to cement the critical

relationships and bonds that we've established with other government (both Federal and State) and private sector entities.

I believe that NPPD needs to continue to attract and retain the skills needed to meet the growing demands of cyber security. As our Nation's dependence on the Internet continues to grow, NPPD needs to continue to evaluate the structure to ensure that we have comprehensive situational awareness and are responsive to the changing demands.

44. Based on your experience as Acting Under Secretary, do you believe that DHS has the proper tools to compel industry and other agencies to respond to the Department's guidance on cyber security issues?

As provided for by the President's National Strategy to Secure Cyberspace and Homeland Security Presidential Directive 7, the National Cyber Security Division (NCSD) serves as a National focal point for addressing cyber security. Collaboration and partnership are key elements for the defense of cyberspace, and the government's leadership role is a critical component of that mission.

Cyber security is a shared responsibility that requires the government and private sector to work in collaboration. While the private sector builds, owns, and operates most of the cyber infrastructure, the Federal Government has the responsibility of ensuring that government functions continue to operate, securing their timely restoration if they fail, and limiting any impact to national security, the economy, public health and safety, and public confidence. Since so many organizations have significant roles in the protection of cyberspace, the key to success is strategic partnering.

45. Do you believe the Department's cyberspace security research and development (R&D) budget is sufficient and appropriate, in comparison to other R&D priorities? What are DHS's current priorities for R&D in the area of cyberspace security?

The Department has a strong cyber security research and development (R&D) program. NCSD develops annual cyber security Research & Development requirements for input into the DHS Science and Technology (S&T) Directorate's cyber security R&D portfolio. Working with the IT Sector through the Sector Coordinating Council and Government Coordinating Council, NCSD identified nine R&D priorities, including cyber situational awareness, cyber forensics, identity management, intrinsic infrastructure protocols security, modeling and testing, control systems security, scalable secure systems, secure coding, software engineering and hardware design improvement, and trust and privacy. NCSD also identified, through a review of the Sector Specific Plans, additional cyber security-related R&D priorities for input to S&T's cyber security R&D portfolio. Additional cyber security R&D priorities included protection, detection and sensor systems, insider threat, emerging technologies, next generation architectures, non-technology security issues, improved cyber attack detection and countermeasures, risk management practices, infrastructure resiliency, and infrastructure dependencies and interdependencies.

46. The Baltimore Sun reported on September 20th of this year about a plan, referred to as the "Cyber Initiative," which reportedly calls for the National Security Agency (NSA) to work with DHS and other agencies to monitor cyber networks. The article states that Director of National Intelligence McConnell is coordinating the effort, but it will be run by DHS.

    a. What is DHS's role in this initiative and what is its current status?

    We will provide the Committee and your staff a classified briefing on this issue.

    b. As Acting Under Secretary, what specifically has your role been in its development?

    We will provide the Committee and your staff a classified briefing on this issue.

    c. What role has Assistant Secretary Garcia played in the development of this initiative?

    We will provide the Committee and your staff a classified briefing on this issue.

    d. When do you believe this initiative will be deployed?

    We will provide the Committee and your staff a classified briefing on this issue.

    e. Once this initiative is deployed what will your role be in its implementation, if confirmed?

    We will provide the Committee and your staff a classified briefing on this issue.

    f. What will the role be of the Assistant Secretary of Cyber Security and Telecommunications in this initiative once deployed?

    We will provide the Committee and your staff a classified briefing on this issue.

    g. Do you anticipate that this initiative will lead to structural chances within the Directorate?

    We will provide the Committee and your staff a classified briefing on this issue.

    h. Will the DNI have management authority over DHS employees for the purposes of this initiative?

    We will provide the Committee and your staff a classified briefing on this issue.

    i. The Baltimore Sun also reports that up to 2,000 people will be involved in this initiative. Is this accurate? Approximately how many DHS employees will be involved?

We will provide the Committee and your staff a classified briefing on this issue.

j. Do you anticipate that this initiative will lead to an increase in the FY 09 budget request for the Directorate? If you anticipate it will, which components will receive the additional funds?

We will provide the Committee and your staff a classified briefing on this issue.

k. Are privacy concerns being considered during the planning stages of this initiative, including for the new responsibilities of NSA?

We will provide the Committee and your staff a classified briefing on this issue.

l. Please provide any additional information relating to this initiative and how it will change DHS's role in protecting cyber infrastructure.

We will provide the Committee and your staff a classified briefing on this issue.

47. Based on your experience as Acting Under Secretary, what do you believe are the critical issues facing control system security? How is DHS addressing these issues?

DHS has three main objectives for reducing cyber risk and securing control systems: provide guidance, develop and enhance partnerships, and prepare for and respond to incidents. The Department also leverages the expertise and activities of operational programs and strategic initiatives from across the Department and the U.S. Government and integrates these activities to reduce risk, respond to incidents, and foster a culture of preparedness within the control systems community.

To address the challenges facing control systems, the Department provides education and training for our industry and government partners on control systems security. In addition, DHS is working with the National Institute of Standards and Technology (NIST) to strengthen Federal standards and guidance regarding control systems security and develop a catalog of control systems security standards.

48. Earlier this year, DHS alerted certain sectors to "the Aurora scenario" vulnerability, which showed that rotating electrical machines could be damaged through a remote cyber attack. This vulnerability – which if exploited could have a severe impact on the electric, nuclear, and water sectors, among others – illustrated the even greater potential risks that exist due to infrastructure components being connected to the Internet.

a. What has been the response so far from the sectors that have been alerted to this vulnerability?

The Department has been collaborating with the public and private sector to develop mitigation strategies since the discovery of the vulnerability. These outreach activities include briefing the affected sectors on the nature of the vulnerability,

convening subject matter experts specific to each sector, and coordinating information sharing between the public and private sector. Outreach activities to the Nuclear and Electric Sectors began in February 2007. The Department engaged the Dams, Locks and Levees Sector in June 2007 and the Chemical, Oil and Gas, and Water Sectors in July 2007. The sectors have been receptive to the mitigation strategies and have begun to implement the recommendations. Additional outreach to the other sectors is ongoing. In addition, DHS briefed 19 control systems vendors on the mitigation plan, through the DHS NCSD Vendors Forum, to prepare them for customer inquiries.

b. Have sectors been complying with the mitigation plans provided by DHS?

The mitigation plans have been rolled out in the Nuclear and Electric Sectors. NCSD is continuing to brief other sectors, including the Oil and Gas Sector and the Water Sector, on the vulnerability. Each of the sector mitigation guidance documents urged that actions be taken within 60 days and then again within 180 days. The Nuclear Regulatory Commission (NRC) issued a letter, coordinated for release along with the Sector's mitigation guidance, requesting that Nuclear Sector licensees provide an update to the NRC on progress made at the completion of the 60-day and 180-day efforts. In this way, the Nuclear Sector took aggressive action to develop and implement mitigations that would reduce the exposure of nuclear power facilities to this vulnerability.

c. What are the Department's next steps in securing this particular vulnerability?

Continued outreach to the sectors as well as the distribution and use of tools such as the Control Systems Cyber Security Self Assessment Tool (CS2SAT) will contribute to securing our critical infrastructure against this particular vulnerability. Through the CS2SAT desktop software, users input facility-specific control system information. The tool then provides users with a picture of their control systems architecture and an assessment of their cyber security posture. It also makes recommendations for improvements. The recommendations are derived from industry cyber security standards and are linked to a set of specific actions that can be applied to mitigate the identified security vulnerabilities. The Instrumentation, Standards and Automation Society, one of the largest global organizations for control systems, announced on October 4, 2007, that it will make the CS2SAT available to their membership, which consists of over 30,000 automation professionals.

Another risk-reduction tool DHS sponsors for the control systems community is the Multi-State Information Sharing and Analysis Center (MS-ISAC) Supervisory Control and Data Acquisition (SCADA) Procurement Project. We have worked closely with the MS-ISAC, the SANS Institute, the Department of Energy Idaho National Laboratory, and representatives from government and industry to develop common procurement language that owners and regulators can incorporate into contracting mechanisms to ensure the control systems they are buying or maintaining have the best available security. The long term goal is to raise the level of control systems

security through the application of robust procurement requirements. The Procurement Project has received very positive feedback from users, and the document has averaged more than 450 downloads per month from the MS-ISAC website where it was posted in January 2007.

The Department also provides education and training for our industry and government partners. Through our control systems security training courses, we have provided training to nearly 7,000 IT and control systems professionals on a range of topics, such as identifying control systems vulnerabilities, conducting risk assessments, and applying standards-based mitigation measures to improve security. We offer both classroom and web-based instruction modules and will be launching a new operations security course later this month. The web-based training has been especially popular with our partners with geographically dispersed systems and personnel.

d. Based on this experience, do you believe the Sector Coordinating Councils are sufficiently able to get critical information out to the sectors?

The National Infrastructure Protection Plan (NIPP) framework and supporting Sector-Specific Plans (SSPs) provide a coordinated approach to critical infrastructure protection roles and responsibilities for Federal, State, local, tribal, international, and industry security partners. Utilizing the NIPP framework and its partnership model of Sector Coordinating Councils and Government Coordinating Councils, DHS directed recent activity to validate and mitigate a control systems vulnerability affecting a number of critical infrastructure sectors. Numerous Federal agency partners worked closely with industry technical experts to assess the vulnerability and to develop sector-specific mitigation plans. This partnership has produced jointly developed mitigation guidance and allowed owners and operators within the affected sectors to take deliberate and decisive actions to reduce significantly the risk associated with this vulnerability.

49. A key component of almost every sector is a reliance on cyber infrastructure.

a. Based on your review, do you believe the Sector Specific Plans have sufficiently addressed cyber security?

Many of the SSPs were created in summer and fall of 2006. Since their development, sectors have been implementing the plans and continuing or initiating efforts to address the security of their cyber infrastructure. Sectors are not uniformly comprehensive in their cyber security efforts and should not necessarily be. Each sector must consider its cyber security posture and balance that against other risk management efforts, in consideration of the unique aspects of its infrastructure. Cyber risk varies by sector, based on the sector's dependence on cyber elements. The more recent organization of some sectors is another factor in the comprehensiveness of their plans.

NCSD is committed to continuing to assist sectors to address cyber security in their SSPs. NCSD will continue to schedule regular interactions with individual sectors as well as meetings with multiple sectors. NCSD will develop guidance on cyber elements that should be considered for inclusion in the SSPs and SARs. NCSD will also work with sectors through their coordinating councils to identify cyber subject matter experts within their sectors and raise awareness of each sector's reliance on cyber infrastructure.

b. What do think the next steps should be to ensure that the sectors are properly taking cyber security vulnerabilities into consideration?

Access to cyber vulnerability information and regular assessment of risk can ensure that sectors are properly considering cyber security vulnerabilities. To obtain access to timely information pertaining to cyber vulnerability information, sectors should encourage individual members to sign up to obtain alerts and bulletins through the National Cyber Alert System and establish relationships with the United States Computer Emergency Readiness Team (US-CERT). Where Information Sharing and Analysis Centers exist for a particular sector, sectors should encourage individual members to join to obtain access to trusted information regarding cyber vulnerabilities, incidents, and mitigation strategies. Sectors should routinely visit the DHS/National Institute of Standards and Technology National Vulnerability Database (NVD), which integrates all publicly available US Government IT vulnerability resources at one easily accessible location.

Also, sectors should assess cyber risk by using the NCSD-developed Cyber Security Vulnerability Assessment (CSVA), a flexible and scalable approach that analyzes an entity's cyber security posture and describes gaps and targeted considerations that can reduce overall cyber risks. It assesses the policies, plans, and procedures in place to reduce cyber vulnerability in 10 categories.

Office of Risk Management and Analysis

50. On March 31, 2007, in conjunction with the reorganization mandated by the Post-Katrina Act, the Secretary established the Office of Risk Management and Analysis, formerly a component of the Office of Infrastructure Protection, as an independent office within the National Programs and Protection Directorate. The stated mission of the Office is to "lead the Department's efforts to establish a common framework to address the overall management and analysis of homeland security risk… serve as the DHS Executive Agent for national-level risk management analysis standards and metrics… (and) develop and embed a consistent, standardized approach to risk and develop a coordinated, collaborative approach to risk management that will allow the department to leverage and integrate risk expertise across components and external stakeholders."

a. How will this office relate to the ongoing risk assessment activities in other components?

The mission of RMA is to coordinate risk analyses across the Department of Homeland Security to ensure all DHS components have access to robust risk methodologies and analytical techniques. RMA will harmonize the definitions of risk analysis terms across the Department, but RMA also recognizes that there is not a one-size-fits-all approach to risk analysis. Analytical techniques will vary depending on the scope and scale of the risk analysis. As such, RMA will maintain an inventory of risk analysis techniques and methodologies and assist the Department components with analyses, as needed. RMA will also lead certain cross-component risk analyses.

b. Given that this office used to be a division of OIP with a focus on critical infrastructure, do you believe it has the necessary experience and credibility to influence the risk assessment approach of the rest of the Department?

RMA is establishing the mechanisms and protocols to reach out and utilize academia, National laboratories and the private sector. These multi-disciplinary pools of experts have strong backgrounds in risk theory, policy, management, methodology development, analysis tools, and modeling techniques. This enables RMA to offer superior quality products and support from the pool of multi-disciplinary experts.

c. What has this office accomplished in the past six months since it was established?

RMA is working collaboratively with the Department's Components to ensure that risk programs are synchronized and integrate sound, systematic principles, utilizing a common approach and lexicon. Since April 1, 2007, RMA has accomplished the following:

1. *Organized and established the Office of Risk Management and Analysis.*
2. *Established the Department's Risk Steering Committee as part of a governance process for risk.*
3. *Initiated the cataloging of Department risk assessment programs.*
4. *Formed and led work groups to refine and improve the risk methodology for analyzing non-NSSE (National Special Security Events) special events.*
5. *Have begun assisting FEMA with the risk methodology build out for the National Preparedness System (NPS).*
6. *Created and implementing a risk lexicon development program.*
7. *Partnered with the Office of National Capital Region, and the State and local members of that region, to assist in the development of a regional risk assessment tool.*
8. *Partnered with Office of Science and Technology (S&T) to assist their Capstone Integrative Process Teams in establishing criteria for addressing the impact of risk on functional capability gaps.*

US-VISIT

51. Earlier this year, as part of DHS's reorganization, the US-VISIT program was placed in NPPD. US-VISIT is intended, in part, to enhance the security of our citizens and visitors

and ensure the integrity of the U.S. immigration system. In so doing, US-VISIT is to record selected travelers entry and exit to and from the United States at over 300 ports of entry around the country, verify their identity, and determine their compliance with the terms of their admission and stay.

a. How is US-VISIT aligned with other NPPD components to accomplish its mission?

Reducing risk requires an integrated approach that encompasses physical and virtual threats, as well as the human elements that pose those threats. Currently, there are multiple components within NPPD working to reduce our comprehensive risk. Three of these are:

- *The Office of Infrastructure Protection (OIP), which addresses physical risks;*
- *The Office of Cyber Security and Communications (CS&C), which addresses cyber risks; and*
- *US-VISIT, which addresses human risks.*

All three of these offices use the same approach to reduce risk by utilizing data gathering, data analysis, and dissemination of information to operators. I believe that we can increase the synergies between, and improve the output of, the aforementioned offices by not only recognizing their commonalities, but also integrating their work more closely.

b. Is the US-VISIT program appropriately located within the NPPD, rather than within a similarly mission-based component such as Customs and Border Protection (CBP)? If so, why?

The mission of CBP is to be the guardian of our Nation's borders. US-VISIT provides the biometric entry and exit program at the border, but also provides services for immigration benefits (U.S. CIS), for the visa application process beyond our borders (State Department), and for law enforcement purposes (ICE and FBI). DHS has recognized US-VISIT's role in protecting the Nation's infrastructure by re-aligning the program into the National Protection and Programs Directorate (NPPD). US-VISIT was placed in the NPPD to support coordination of the program's protection mission and to strengthen management oversight. The placement of US-VISIT into this new Directorate recognizes that US-VISIT has evolved from a border control program created to address specific legislative mandates to an organization that is now an asset for the entire Department.

c. Can you clarify NPPD's role in ensuring that US-VISIT develops and implements a workable plan for implementing a biometric exit capability? What will NPPD do to hold US-VISIT accountable for deploying a biometric exit capability?

NPPD has provided oversight to the development of this strategy from the time US-VISIT was first made a part of the Directorate. I meet with the Director of US-VISIT daily to discuss critical issues; we meet at least weekly in an extended session to discuss a variety of issues including exit strategy and to coordinate and provide guidance on issues critical to the Department.

As Comprehensive Exit has developed, NPPD has required reports from US-VISIT, such as the weekly Project Status Report, and has helped US-VISIT to overcome challenges. We will continue to require reports and will supplement that by frequent meetings between the Director of US-VISIT and the Under Secretary of NPPD.

d. How will you ensure that US-VISIT has sufficient accountability and common performance measures in order to address its immigration enforcement role in conjunction with CBP and Immigration and Customs Enforcement?

In response to my request, US-VISIT has developed improved performance measures. These measures explain US-VISIT's contributions to security based upon three constructs: accuracy, responsiveness, and efficiency. Measures related to accuracy assist the program in assessing the quality of information provided to stakeholders and calibrating our processes and systems to better support improved risk and eligibility decisions. The responsiveness measures allow the program to determine whether the information being provided to stakeholders meets their needs for timely decision-making within their business processes and rules. Efficiency measures facilitate program management's efforts to increase identity and document verification capabilities while simultaneously targeting resources for optimal yield and being responsible stewards of taxpayer dollars.

52. According to a February 2006 GAO report, border security program officials did not always have the information they needed to anticipate problems such as processing high volumes of visitors in space constrained facilities, in part because the approach taken by the US-VISIT program office to evaluate its impact on land port of entry facilities focused on paperwork processing times and not on other operational factors like the impact on physical facilities. Can you tell us your strategy for addressing ongoing programmatic problems that have been identified with the US-VISIT program?

Under my leadership, US-VISIT has worked to develop a timeline to meet all GAO recommendations. This effort has been briefed to GAO and they approve of the way forward. Currently US-VISIT evaluates the operational impact of changes to primary and/or secondary processes as a result of any US-VISIT initiative. These impacts may include traveler wait times, physical infrastructure, and /or CBP staffing.

53. An August 2007 GAO report on the Department's progress in implementing its missions and functions found that DHS has not yet implemented a program to detect and identify illegal border crossings between ports of entry. Part of GAO's concern is the lack of clarity about whether the Secure Border Initiative (SBI) and SBInet will be linked to the US-VISIT Program in order to allow the two systems to share technology, infrastructure, and data. What steps will you take to ensure that US-VISIT is strategically aligned to work in combination with other border security initiatives that are managed by CBP, such as the SBI?

US-VISIT and Secure Border Initiative (SBI) work to complement each other and prevent redundancies. For example, IDENT, the Automated Biometric Identification System,

supports both US-VISIT entry as well as Border Patrol. Another example is that needs identification for communication infrastructure to a point of entry considers input from both US-VISIT and SBI.

54. Congress recently enacted the Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53). Included in that legislation were security enhancements to the Visa Waiver Program and a limited expansion of program. The Secretary of Homeland Security is provided waiver authority to allow additional countries into the Visa Waiver Program upon certification by the Secretary to Congress that there is an air exit system in place to verify the departure of not less than 97 percent of foreign nationals who exit by air. The goal is to ensure that this exit system is fully biometric by June 30, 2009 or the Secretary's waiver authority will be suspended. What do you see as the Department's most significant challenge in implementing a biometric air exit system? Do you believe DHS will be able to meet the June 30, 2009 deadline?

    To be successful, the proposed solution will require active participation by all air and sea carriers. We believe the Air/Sea Exit System can be operational by December 31, 2008, which is the operational date projected in the project schedule.

CFIUS

55. The Committee on Foreign Investment in the United States (CFIUS) is an inter-agency group that is responsible for reviewing any mergers, acquisitions or takeovers of any companies engaged in interstate commerce in the U.S. to determine if there is credible evidence that a foreign investment in that company will impair national (including homeland) security. Though CFIUS is led by the Treasury Department, DHS is one of several other Departments which play a critical role in the process. The Foreign Investment and National Security Act of 2007 (P.L. 110-49), which was signed into law on July 26, 2007, clarifies that CFIUS has the authority to review transactions involving critical infrastructure. DHS has recently expanded its office within the Policy Directorate that is responsible for reviewing these types of transactions; however several additional component agencies and offices play critical roles in reviewing them for national and homeland security implications.

    How will NPPD work with the Policy Directorate to evaluate the risk to homeland security posed by these transactions?

    The DHS Office of Policy has overall responsibility for the Department's CFIUS-related reviews and for making recommendations to the Secretary on how to approach each case. However, dedicated staff from OIP's HITRAC support Departmental decision making by preparing risk assessments of every filing that are provided directly to the Office of Policy. These assessments, prepared by a special CFIUS Support Team of OIP and I&A analysts within HITRAC, provide policy makers within the Department with an understanding of how these acquisitions can impact U.S. infrastructure.

The final risk assessment informs the Office of Policy's recommendation to the Secretary by highlighting areas of increased risk and proposing potential mitigation strategies the Department can use to manage any risk posed by the transaction. Under the Department's Chief Intelligence Officer Charlie Allen's leadership, HITRAC's assessments also inform the Director of National Intelligence's reviews of each CFIUS case, in collaboration with the rest of the intelligence community.

HITRAC continues to provide analytical support and advice to the Office of Policy during negotiations on mitigation agreements that the U.S. Government uses, in some cases, to manage risk. It should be noted that HITRAC produces its assessments in a very compressed timeframe to allow policymakers maximum time to take appropriate actions within the statutory 30-day timeframe mandated for initial CFIUS reviews.

The Office of Infrastructure Protection and HITRAC recognize that thorough scrutiny of the potential risks posed by foreign ownership of critical infrastructure is vital to protecting the Nation's security and economic strength. We will continue to closely monitor CFIUS cases for the emergence of adverse trends, and we will continue to work with our Federal partners to ensure that performance of this mission meets with the highest standards.

V. Relations with Congress

56. Do you agree, without reservation, to respond to any reasonable summons to appear and testify before any duly constituted committee of the Congress if you are confirmed?

Yes.

57. Do you agree, without reservation, to reply to any reasonable request for information from any duly constituted committee of the Congress if you are confirmed?

Yes

VI. Assistance

58. Are these answers your own? Have you consulted with DHS or any interested parties? If so, please indicate which entities.

These answers are my own. I have consulted with the Department on all entries.

AFFIDAVIT

I, Robert D. Jamison, being duly sworn, hereby state that I have read and signed the foregoing Statement on Pre-hearing Questions and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

Robert D. Jamison

Subscribed and sworn before me this 30th day of October, 2007.

Karen R. Williamson
Notary Public

Karen R. Williamson
Notary Public, District of Columbia
My Commission Expires 2/28/2011

United States
Office of Government Ethics
1201 New York Avenue, NW., Suite 500
Washington, DC 20005-3917

September 20, 2007

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510-6250

Dear Mr. Chairman:

In accordance with the Ethics in Government Act of 1978, I enclose a copy of the financial disclosure report filed by Robert D. Jamison, who has been nominated by President Bush for the position of Under Secretary for National Protection and Programs, Department of Homeland Security.

We have reviewed the report and have also obtained advice from the Department of Homeland Security concerning any possible conflict in light of its functions and the nominee's proposed duties. Also enclosed is a letter dated September 14, 2007, from Mr. Jamison to the agency's ethics official, outlining the steps he will take to avoid conflicts of interest. Unless a specific date has been agreed to, the nominee must fully comply within three months of his confirmation date with the actions he agreed to take in his ethics agreement.

Based thereon, we believe that Mr. Jamison is in compliance with applicable laws and regulations governing conflicts of interest.

Sincerely,

Marilyn L. Glynn
General Counsel

Enclosures

Senator Joseph I. Lieberman
Additional Questions for the Record
Nomination Hearing of Robert D. Jamison
November 9, 2007

1. The Department last week finalized the list of chemicals that will trigger potential regulation under the new chemical site security program. While it is encouraging to see the Department making progress on implementing the program, there are ongoing concerns that program may not be as extensive or rigorous as it needs to be. There are concerns that the Department may have gone too far in adjusting certain chemical thresholds to meet industry concerns. More generally, this program remains underfunded and appears to be too reliant on contractors, some of whom may reflect an industry bias.

   a. How do you plan to secure the resources and in-house expertise to ensure that this vital program provides robust and effective regulation of the chemical security risk?

      While the stand up of the Chemical Facility Anti-Terrorism Standards (CFATS) program presents many challenges, the Chemical security program is a top priority of the National Protection and Programs Directorate. I plan to ensure implementation of the various phases of the CFATS program. Working with the Chief Financial Officer as well as the leadership at the Department, I will continue to monitor the demands on the program to ensure we have the proper resources to carry out our mission. I have also directed the stand up of a Human Capital Taskforce to ensure that we are attracting top notch talent across the Directorate, including the key positions for the CFATS program. Finally, we must continue to re-baseline as we receive information from our top screening efforts. Based upon the risks identified during this process, we must ensure we are properly resourced to reduce risk in the chemical sector.

   b. The current statutory authority is circumscribed in certain respects, for instance there is no ability to regulate water facilities that may use extensive amounts of hazardous chemicals. Does the Department plan to advocate for broader authorities, as Secretary Chertoff has suggested it might?

      I will be working closely with the chemical security team as we continue to examine the issue of water facilities. We recognize that the chemicals like chlorine, which is used by water facilities, pose a serious security threat. We have already taken action to address threats from chlorine, both from the toxic release and the theft and diversion perspective. For example, chlorine is listed as a "Chemical of Interest" on the recently released final rule Appendix A to the chemical security program. Water facilities however, are exempt from the chemical security program. So the Department has aggressively reached out to these facilities, working with both the Sector Specific Agency, the Environmental Protection Agency, and the Drinking Water and Water Treatment Sector to assess and advise on security best practices.

The Department remains determined to protect the country from high-risk chemical threat, and will continue to work closely with the Sector.

c. In the recently released list of chemical thresholds, the Department justifies an increase in the threshold amount of chlorine by noting the extensive use of chlorine throughout the economy. While the widespread use of chlorine and other dangerous chemicals poses certain practical constraints in terms of regulation, it is hardly reassuring in terms of the risk we face from potential misuse of these chemicals. For this reason, do you agree that the Department should be encouraging the use of safer technologies and processes wherever possible – including substitution? If so, how will the Department's chemical security program promote this goal?

The Department's overarching mission is to manage risk to the Nation and we believe that the CFATS approach promotes risk reduction in a way that wil make the Nation safer and more secure. We believe that the completion of the top screen, as will be required when Appendix A to CFATS publishes in the Federal Register, is an essential first step in evaluating risk on a national level. The requirement to complete the top screen is key as it will allow us to build a data set regarding potentially high risk facilities that does not exist at this time.

Second, it is important to continue the ongoing efforts by industry to reduce risk. The CFATS process will validate protective measures in place, including, measures that sufficiently reduce risk in a way that meet the risk-based performance standards of the program. CFATS provides that all regulated facilities will be sorted into Tiers. The requirements for an owner-operator become increasingly significant (and costly to implement) as the Tier level goes up. Risk reduction measures are entirely within the discretion of the owner-operator, however, as a practical matter, the first consideration at the higher risk facilities will be to reduce consequence. As we have said before, the CFATS program is not at all a "one size fits all" set of requirements, rather, it is designed to ensure a layered set of protective measures appropriate to secure a particular high risk facility. The Department will be reviewing facility security plans and approving them if they adequately reduce the risk presented to that particular facility.

2. The National Programs and Protection Directorate was created as part of the Department's reorganization after Hurricane Katrina. NPPD does not appear to be organized around a central theme or mission, which may cause management challenges and impede each of its comprising offices' abilities to accomplish their unique missions. For example, US-VISIT is separated from the customs and immigration agencies and the Risk Management Office might be more effective if its location facilitated coordination across the Department, such as the Policy Directorate.

   a. Based on your experience as Acting Under Secretary of NPPD for the past seven months, please describe what you believe your principal mission to be.

As you note, the Directorate has a diverse operating mission that ranges from cyber security to delivery of biometric identity services. The past seven months have shown me that the tie that binds each of these unique offices is our common mission of risk reduction. I am leading a team of individuals that is working daily to drive down risk across our areas of responsibility. We must continue to build on our efforts of the past seven months to leverage our resources and work as a team to move forward to build a strong and stable Directorate.

b. Have you found the organization of the Directorate to be an asset or impediment? Please explain why.

The organization of this Directorate is an asset. As I noted in my earlier answers our core strength and one of our biggest assets is the dedicated, loyal, and mission-focused staff. We will continue to leverage our individual strengths as well as those our components (e.g., US-VISIT's expertise in project management and information technology are applicable across parts of the Directorate) to make the Directorate stronger as a whole.

3. If confirmed, you will have a little over a year in your position to effectuate change at the Department. When you leave the Department in January 2009, what is the most important thing you hope to have accomplished?

As I noted in my answer to question 15, there are two primary focus areas for me: 1) the maturation of the Directorate and 2) meeting key milestones in our most important programs.

My top priorities in terms of maturation of the Directorate are: a) attracting and retaining the skills sets needed to advance these programs and successfully navigate the transition of administration; b) fostering improved teamwork across the Directorate and leverage the diverse skills across the individual components; and c) improving the fundamental business practices across the Directorate.

I will also focus on meeting key milestones to successfully implement a) the Chemical Facility Anti-Terrorism Standards Regulation; b)US-VISIT's Air Exit regulation; and c) improved cyber security defense across the Federal government.

4. The Office of Risk Management and Analysis (RMA), which was established earlier this year within NPPD, is tasked with establishing a common framework across the Department for analyzing and managing homeland security risk. The question of how risk should be calculated is a challenge for all components of the Department, and certainly efforts to standardize and consolidate that process are laudable. However, given that the RMA has a very small staff and is buried within NPPD, it is unclear to me that this office has the ability to lead this effort.

a. How will the Office of Risk Management and Analysis affect the risk assessment activities in other DHS components?

The Office of Risk Management is leveraging risk management expertise across all of the DHS components through the Risk Steering Committee. The Department Risk Steering Committee, established and managed by RMA, includes three tiers; component principals (Tier I), sub-component principals (Tier II), action officers (Tier III), and an Executive Steering Committee. The Risk Steering Committee process provides the framework for enabling collaboration and Department-wide agreement on risk management efforts. Since April, staff level working groups have been engaged on coordinating risk activities.

b. Given that DHS has taken the position that there is not a "one size fits all" approach to risk analysis, how will the RMA standardize or harmonize the varying methodologies across the Department?

Different types of risk analyses require different methodologies and approaches. A risk analysis focused on grant allocation will have a different analytical approach then a risk analysis focused on infrastructure protection. The role of RMA will not be to create a single approach for all risk analysis but instead to inventory different types of acceptable analytical approaches to develop a common risk lexicon. RMA will identify the various types of risk tools in use throughout the Department, in academia and industry; and will identify what types of problems to which these tools are most applicable. RMA will work with the components to select the tools (e.g., fault tree analysis and simulation models) most appropriate for their analytical needs. RMA will also disseminate information promoting a common risk lexicon that provides components with definitions of risk terms, consequence scales, and reference sources. The ultimate goal is to facilitate the comprehensive evaluation of risk across DHS.

c. What specific products or accomplishments do you hope to see from the RMA over the course of the next year?

RMA will continue efforts on the following through FY08:

- *Production of a guidance document and lexicon for risk based decision making.*
- *Development of a strategic plan for integrating current risk evaluation methodologies into a format that allows broader use of the information to make informed decisions.*
- *The development of a risk methodology to assist the Department's Chief Financial Officer with the application of risk in Future Year Homeland Security Programming.*

5. In testimony before this committee in September, GAO reported that DHS lacked a means for measuring performance in most components of the Department. You have said that implementing metrics to measure success is a priority for you. However, achievements in certain programs in NPPD are more easily measured than others.

a. Please discuss how you intend to implement outcome-based metrics across the Directorate.

The directorate has already started what will become an ongoing effort to determine the appropriate outcome based measures that would calibrate our management efforts to improve performance. It is important to build a culture where the organization understands its mission and is confident enough to measure the right outcomes that may not be 100% in their control. The first step is understanding what you are trying to accomplish. The next steps are setting appropriate metrics that are measurable and that capture the performance of the unit. You must also drive improvements through your management structure. It takes communication, training, and a commitment by senior management to build the culture. I am committed to building that culture in NPPD.

b. Is this achievable in the Office of Infrastructure Protection, for example, where success comes from sharing information and collaborating with the private sector as opposed to producing specific deliverables? How do you measure information sharing for example?

As we embark on the effort to improve how we measure security in the field, we must strive to ensure that we build upon the collaborative spirit of the NIPP framework. Achieving the balance of ensuring that the 17 sectors are continuing to implement sound security measures and drive down risk, while maintaining the free flow of information between government and our partners is a challenge. It is a challenge that is worth taking on to ensure that our critical infrastructure is secure.

Measuring information sharing is a good example that illustrates an important distinction between outcome measures and output measures. Some have tried to measure results by the number of products produced, the number of conference calls conducted, or other output measures. Another indicator of the quality of information sharing could be the amount of activity on our information sharing HSIN portals. That would give you a good indication of the quality of the products that you are sharing and how relevant they are to your intended audience. You would then strive to improve the products or approach to ensure that you are getting the "market share" that would indicate the dissemination of critical information. As we mature, we plan to implement such a metric.

6. In your answers to the Committee's pre-hearing questions, you stated that "contractors were not asked to draft answers to any of the pre-hearing questions.... However... source materials that were likely drafted by contractors were used at the beginning of the drafting exercise for five questions (44, 45, 47, 48, 49)."

a. Please define what you mean by the term "source document."

The term "source documents" refers to text and materials that had been previously prepared. These include: Information Technology Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (May 2007); Statement for the Record Gregory Garcia, Assistant Secretary for

Cybersecurity and Communications, National Cyber Security Division, U.S. Department of Homeland Security, Before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity and Science and Technology (October 17, 2007); Statement for the Record Gregory Garcia, Assistant Secretary for Cybersecurity and Communications, National Cyber Security Division, U.S. Department of Homeland Security, Before the U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Policy, Census, and National Archives (October 23, 2007); Statement for the Record Gregory Garcia, Assistant Secretary for Cybersecurity and Communications, National Cyber Security Division, U.S. Department of Homeland Security, Before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Emerging Threats, Cybsecurity, and Science and Technology and the Subcommittee on Transportation Security and Infrastructure Protection (October 31, 2007); Questions for the Record, Senate Homeland Security and Governmental Affairs Federal Financial Management, Government Information, and International Security Subcommittee "Cyber Security: Recovery and Reconstitution of Critical Networks" (July 28, 2006) Under Secretary George Foresman; Questions for the Record, U.S. House of Representatives, Committee on Appropriations Hearing Date: March 20, 2007.

b. Were the source documents referred to in your answer drafted after you received the pre-hearing questions from the Committee or were they pre-existing documents?

No, the source documents were pre-existing documents.

c. Was the explicit purpose of drafting the source documents to assist in answering the Committee's pre-hearing questions?

No, the source documents were pre-existing documents.

d. How did you verify that no contractors were asked to draft answers to the pre-hearing questions?

I directed my Acting Chief of Staff, Jeanette Hanna-Ruiz, to initiate an inquiry on whether contractors were used to answer any pre-hearing questions. Ms. Hanna-Ruiz met with my direct reports: Bob Stephan, Tina Gabbrielli, Robert Mocny, Anne Petera, and Hun Kim (an SES member who was present for Greg Garcia) and requested that each of them review the draft answers they submitted in response to the pre-hearing policy questions and determine whether there was any contractor involvement. Ms. Hanna-Ruiz reported to me that all but one of my direct reports confirmed that no contractors were used in drafting the draft answers to the pre-hearing policy questions they submitted. She followed up with Greg Garcia and his staff to determine which questions may have had some contractor input. During this inquiry, it was discovered that two contractors in the National Cyber Security

Division (NCSD) had participated in the development of responses using pre-existing source materials to respond to a small set of questions.

Please see the attached timeline that details our process for verifying that no contractors were asked to draft answers to the pre-hearing questions.

e. Please describe all instances in which the Committee's questions were provided to contractors in order to assist in the preparation of answers. Include in your answer a list of all the questions provided to contractors, and identify the contractors involved in drafting or preparing documents or other materials in response to each of the questions?

Questions were disseminated to Bob Stephan, Tina Gabbrielli, Robert Mocny, Greg Garcia, and Meghan Ludtke by the NPPD Acting Chief of Staff with the explicit direction that "these questions should only be forwarded to SES level division directors." In the case of questions 39, 44, 45, 47, 48, 49, the Acting Director of the National Cyber Security Division (NCSD) did not fully adhere to this request[1]*. As a result of several circumstances (e.g., the government employee who handles policy was out of the country and the urgent timeline for response), the Acting Director asked two front office executive secretariat contractor staff to cull responses from previously prepared source materials in the NCSD records archive. This is a standard practice in the NCSD to leverage pre-existing work product and to ensure the most efficient use of staff resources. The pre-existing source documents were developed with a mixture of input from both government and contractor staff.*

Once a preliminary draft was compiled for these questions from the pre-existing source materials, the NCSD Acting Director then reviewed and edited the responses for currency and accuracy and submitted them to the Office of Cybersecurity and Communications (CS&C) for further review. The responses then underwent additional review and editing by government personnel in CS&C who submitted them to NPPD. Government personnel at the Directorate-level in NPPD then further revised the responses prior to me making edits before their final submission to the Committee.

The two contractors assisting with this task work in the Executive Secretariat of CS&C and provide full time, onsite support to the NCSD at the DHS Glebe Road facility.

The questions provided to the two contractors were as follows.

> *39) In June 2006, DHS concurred with GAO's recommendation that the Department review the National Communications System and National Cyber Security Division organizational structures and roles to address the convergence of the voice and data communications. On October 1, 2007, Assistant Secretary*

[1] On further inspection of records, it was discovered that question 39 had also been provided to two contractor staff in the National Cyber Security Division.

Greg Garcia stated: "With the convergence of the IT and communications sectors, we need to ensure synchronized information sharing and response capabilities across our communications and cyber networks, precisely because those networks are becoming one and the same."

a. *What is DHS doing to ensure that this information sharing across networks is occurring?*
b. *If confirmed, how will you reorganize DHS components to deal with the convergence of voice and data communications?*

44) Based on your experience as Acting Under Secretary, do you believe that DHS has the proper tools to compel industry and other agencies to respond to the Department's guidance on cyber security issues?

45) Do you believe the Department's cyberspace security research and development (R&D) budget is sufficient and appropriate, in comparison to other R&D priorities? What are DHS's current priorities for R&D in the area of cyberspace security?

47) Based on your experience as Acting Under Secretary, what do you believe are the critical issues facing control system security? How is DHS addressing these issues?

48) Earlier this year, DHS alerted certain sectors to "the Aurora scenario" vulnerability, which showed that rotating electrical machines could be damaged through a remote cyber attack. This vulnerability – which if exploited could have a severe impact on the electric, nuclear, and water sectors, among others – illustrated the even greater potential risks that exist due to infrastructure components being connected to the Internet.

a. *What has been the response so far from the sectors that have been alerted to this vulnerability?*
b. *Have sectors been complying with the mitigation plans provided by DHS?*
c. *What are the Department's next steps in securing this particular vulnerability?*
d. *Based on this experience, do you believe the Sector Coordinating Councils are sufficiently able to get critical information out to the sectors?*

49) A key component of almost every sector is a reliance on cyber infrastructure.

a. *Based on your review, do you believe the Sector Specific Plans have sufficiently addressed cyber security?*
b. *What do think the next steps should be to ensure that the sectors are properly taking cyber security vulnerabilities into consideration?*

f. Please provide the Committee with all documents or other materials that were drafted or prepared by contractors and used to help answer your pre-hearing questions. Identify in each case who prepared the documents or other materials and whether the documents or materials were prepared in response to the questions.

The documents listed below were used as source documents for the development of answers to pre-hearing questions 39, 44, 45, 47, 48 and 49.

- *Attachment 1- IT Sector Specific Plan, May 2007. The document was jointly developed in public private partnership by Government and industry representatives. It was not developed to respond to the pre-hearing questions.*

- *Attachment 2- Statement for the Record of Gregory Garcia, Assistant Secretary for Cybersecurity and Communications, DHS, before the United States House of Representatives Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, October 17, 2007. The document was developed by government and contractor personnel in the Office of Cybersecurity and Communications. It was not developed to respond to the pre-hearing questions.*

- *Attachment 3- Statement for the Record of Gregory Garcia, Assistant Secretary for Cybersecurity and Communications, DHS, before the U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Policy, Census and National Archives, October 23, 2007. The document was developed by government and contractor personnel in the Office of Cybersecurity and Communications. It was not developed to respond to the pre-hearing questions.*

- *Attachment 4- Statement for the Record of Gregory Garcia, Assistant Secretary for Cybersecurity and Communications, DHS, before the United States House of Representatives Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology and the Subcommittee on Transportation Security and Infrastructure Protection, October 31, 2007. The document was developed by government and contractor personnel in the Office of Cybersecurity and Communications. It was not developed to respond to the pre-hearing questions.*

- *Attachment 5- Response to Questions for the Record to the Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Federal Financial Management, Government Information, and International Security hearing on "Cyber Security: Recovery and Reconstitution of Critical Networks", July 28, 2006. The document was developed by government and contractor personnel in the Office of Cybersecurity and Communications. It was not developed to respond to the pre-hearing questions.*

- *Attachment 6- Response to Questions for the Record to the U.S. House of Representatives Committee on Appropriations hearing on the DHS National Programs and Protection Directorate and Infrastructure Protection, March 20, 2007. The document was developed by government and contractor personnel in the Office of Cybersecurity and Communications. It was not developed to respond to the pre-hearing questions.*

g. Please list any other instances in which contractors assisted in the process of responding to your pre-hearing questions.

There are no other instances in which contractors assisted in the process of responding to pre-hearing questions.

Timeline

To the best of my recollection the timeline below is my most accurate representation of the events that have transpired in response to the pre-hearing policy questions for Robert D. Jamison:

1. Friday, October 19, 2007 12:34 pm
    a. Email from David Hess to Jeanette Hanna-Ruiz, Kristina Dorville, Elizabeth Gary, Robert Jamison, Lee Morris, Timothy Johnson, Erin White and David Hess
        i. The email attached all pre-hearing policy questions for Robert D. Jamison nomination requesting they be turned around as soon as possible; noting the need for DHS OGC review and final approval and transmittal to Committee.
2. Friday, October 19, 2007 – late afternoon core group staff meeting in the office of Jeanette Hanna-Ruiz with: Kristina Dorville, Elizabeth Gary, and Jeanette Hanna-Ruiz and David Hess via telephone.
    a. A discussion took place on how we should handle the pre-hearing policy questions. Three options were suggested at that time: 1) answer all the questions ourselves, 2) spend one day in a war room with key government staff and answer all the questions, or 3) send the questions out to Robert's direct reports (Director, Acting Director, and A/S level personnel) for them to answer with SES level personnel from their divisions. After a brief discussion we agreed that alternative 3 was the optimum way forward.
3. On Friday October 19, 2007 at 4:37 I received an email from David Hess. It was addressed to: Jeanette Hanna-Ruiz, Kristina Dorville, Elizabeth Gary, Robert Jamison with a CC of Lee Morris, Timothy Johnson, Kristin Royster, Erin White, and David Hess.
    a. The email was addressed to the National Protection and Programs Directorate Office of the Under Secretary ("NPPD OUS"). It asked if the pre-hearing policy questions had been sent out to NPPD divisions.
4. On Friday, October 19, 2007 at 5:09 pm I, Jeanette Hanna-Ruiz, sent an email to Robert Mocny, Bob Stephan, Greg Garcia, Tina Gabbrielli, and Anne Petera with a CC to Elizabeth Gary, Kristina Dorville and David Hess.
    a. The subject of the email was "Policy Questions". The emailed stated that the policy questions for Robert's hearing had arrived and that I would be sending them out to them and their CoS. The email gave a due date of COB 10/23/07. The emailed stated in **bold "These questions should only be forwarded to SES level division directors." It requested that once all answers were compiled that they be forwarded to me.**
5. On Friday October 19, 2007 at 5:11 pm I sent forward the 10/19/07 5:09 pm email noted above to: to Penelope Smith, US-VISIT; Sue Armstrong, Infrastructure Protection; Hun Kim, Cyber Security and Communications; and Eric Tysarczyk. The emailed stated: "PLEASE SEE BELOW. Please not *sic* note the limitation on who should be answering these questions."

   a. 11/10/07 12:48 pm I discovered a typo in this email that I left off the e on note in the email above. The email should read: "PLEASE SEE BELOW. Please *note* the limitation on who should be answering these questions."

6. On Friday, October 19, 2007 at 5:16 pm I sent an email to Bob Stephan and Sue Armstrong. The subject of the email was IP policy questions due COB 10-23-07.
   a. This email referenced the 10/19/07 5:09 email noting in **bold that "These questions should only be forwarded to SES level divisions directors."**
7. On Friday, October 19, 2007 at 5:19 pm I sent an email to Greg Garcia and Hun Kim. The subject of the email was CS&C policy questions.
   a. The email referenced the 10/19/07 5:09 email noting in **bold that "These questions should only be forwarded to SES level divisions directors."**
8. On Friday, October 19, 2007 at 5:21 pm I sent an email to Tina Gabbrielli and Scott Breor. The subject of the email was RMA policy questions.
   a. The email referenced the 10/19/07 5:09 email noting in **bold that "These questions should only be forwarded to SES level divisions directors."**
9. On Friday, October 19, 2007 at 5:23 I sent an email to Robert Mocny and Penelope Smith. The subject of the email was US-VISIT Policy Questions.
   a. The email referenced the 10/19/07 5:09 email noting in **bold that "These questions should only be forwarded to SES level divisions directors."**
10. On Friday, October 19, 2007 at 5:23 I sent an email to Robert Mocny and Penelope Smith. The subject was US-VISIT policy questions.
    a. Having discovered that I inadvertently sent them the wrong set of questions I asked them to "disregard".
11. On Friday, October 19, 2007 at 5:26 pm I sent an email to Robert Mocny and Penelope Smith. The subject was "US-VISIT Policy Questions (PLS USE THIS VERSION)."
    a. The email referenced the 10/19/07 5:09 email noting in **bold that "These questions should only be forwarded to SES level divisions directors."**
12. On Friday, October 19, 2007 at 5:28 pm I sent an email to Meghan Ludtke. The subject of the email was legal questions.
    a. The email referenced the 10/19/07 5:09 email noting in bold that "**These questions should only be forwarded to SES level divisions directors."**
13. On Friday, October 19, 2007 at 5:28 pm I sent an email to Tina Gabbrielli and Scott Breor. The subject was RMA policy questions.
    a. Realizing I had addressed the email I sent to Tina as "sir" I apologized and corrected it to "Mam".
14. On Friday, October 19, 2007 at 5:41 pm I responded to the emailed addressed to "NPPD OUS" that I received from David Hess on 10/19/07 at 4:37 pm.
    a. The emailed from David Hess asked if the questions had been sent out. I responded that the hearing questions had been sent out with a deadline of COB Tuesday.
15. On Friday, October 19, 2007 at 5:42 pm I received an email from Meghan Ludtke asking that I meant by SES level division directors.
16. On Friday, October 19, 2007 at 5:44 pm I responded to the email from Meghan Ludtke stating that, "We only want senior level people answering these questions. Does that help."

17. On Friday, October 19, 2007 at 5:50 pm I received an email from Anne Petera regarding the policy questions.
    a. She was asking if I had sent them out already because she had not received any.
18. On Friday, October 19, 2007 at 5:52 I responded to 5:50 pm email from Anne Petera.
    a. I let Anne know that I double checked and she did not have any questions in her area as far as I could tell.
19. On Friday, October 19, 2007 at 5:53 pm I received an email from Anne Petera acknowledging she did not have any policy questions that needed to be answered.
20. On Saturday, October 20, 2007 at 3:55 pm I received an email from Robert Mocny asking for clarification of what is meant by SES level only.
21. On Saturday, October 20, 2007 at 4:46 pm I responded to Robert Mocny's email noting that the questions should not be distributed to a lot of staff and that we were looking for Robert Mocny to coordinate with his senior level staff or division heads.
22. On Saturday, October 20, 2007 at 5:40 I received an email from Robert Mocny acknowledging the guidance on distribution.
23. On Sunday, October 21, 2007 at 2:24 pm I received an email from Meghan Ludtke stating that we had language to answer the questions send to her from testimony before the House Homeland Security Committee in March re: CFIUS.
24. On Sunday, October 21, 2007 I acknowledged receipt of Meghan's 10/21/07 2:24 pm email.
25. On Monday, October 22, 2007 at 12:26pm I received an email from David Hess addressed to Jeanette Hanna-Ruiz and Kristina Dorville with a CC to Kristin Royster.
    a. The emailed contained the pre-hearing policy question answers of Julie Myers.
26. On Monday, October 22, 2007 at 1:16pm I acknowledged receipt of the 10/22/07 12:26 email from David Hess.
27. On Monday, October 22, 2007 at 5:26 pm I received an email from Meghan Ludtke responding to the CFIUS questions which was pulled from previously cleared "ASIP" (Assistant Secretary of Infrastructure Protection) testimony.
28. On Tuesday, October 23, 2007 at 9:04 am I sent out an email to Greg Garcia, Robert Mocny, Anne Petera, Tina Gabbrielli, Meghan Ludtke, and Bob Stephan. The subject of the email was "reminder".
    a. The emailed asked that I received all responses to policy questions by COB.
29. On Tuesday, October 23, 2007 at 9:04 am I received an email from Meghan Ludtke asking me what I was referring to in my 10/23/07 9:04 am email.
30. On Tuesday, October 23, 2007 at 9:05 am I responded to Meghan's 10/20/07 9:04 email letting her know it was the CFIUS materials she had already sent me.
31. On Tuesday, October 23, 2007 at 10:26 am I received an email from David Hess asking when the internal deadline for answering the policy questions.

32. On Tuesday, October 23, 2007 at 3:26 pm I sent out an email to Hun Kim, Lee Stubbs, Penelope Smith, Scott Breor, and Sue Armstrong reminding them that all answers to policy questions were due COB.
33. On Tuesday, October 23, 2007 at 5:34 pm I received an email from Penelope Smith. Attached to the email were US-VISIT responses to the policy questions.
34. On Tuesday, October 23, 2007 at 5:37 pm I sent an email to Bob Stephan, Tina Gabbrielli and Greg Garcia asking them to please submit their policy questions.
35. On Tuesday, October 23, 2007 at 5:55 pm I sent an email to Tina Gabbrielli asking here where the policy questions were.
36. On Tuesday, October 23, 2007 at 5:55 pm I sent an email to Greg Garcia asking here where the policy questions were.
37. On Tuesday, October 23, 2007 at 5:56 pm I sent an email to Bob Stephan asking here where the policy questions were.
38. On Tuesday, October 23, 2007 at 5:56 pm I sent forwarded the 10/23/07 5:56 email to Bob Stephan email to Sue Armstrong asking her where we stood on answering the questions.
39. On Tuesday, October 23, 2007 at 5:56 pm I sent forwarded the 10/23/07 5:55 email to Greg Garcia email to Bruce Landis asking him where we stood on answering the questions.
40. On Tuesday, October 23, 2007 at 5:56 pm I sent forwarded the 10/23/07 5:55 email to Tina Gabbrielli email to Scott Breor asking him where we stood on answering the questions.
41. On Tuesday, October 23, 2007 at 6:02 pm I received an email from Greg Garcia; CCed were John Denning and Bruce Landis. He attached CS&C responses.
42. On Tuesday, October 23, 2007 at 6:03 pm I received an email from Greg Garcia letting me know that John Denning was completing a review/merge of answers and I would have them in an hour.
43. On Tuesday, October 23, 2007 at 6:04 pm I received an email from Sue Armstrong; Christopher Krebs was also in the addressee line. She asked I be sent the answers.
44. On Tuesday, October 23, 2007 at 6:14 pm I received an email from Tina Gabbrielli with the RMA answers.
45. On Tuesday, October 23, 2007 at 6:58 pm I received an email from Bob Stephan asking if I had touched based with Sue who was passing answers to me.
46. On Tuesday, October 23, 2007 at 7:01 pm I received an email from Christopher Krebs stating I would be receiving the answers momentarily.
47. On Tuesday, October 23, 2007 at 7:01 pm I sent an email to Sue Armstrong and Christopher Krebs asking where the answers to the IP questions were.
48. On Tuesday, October 23, 2007 at 7:02 pm I sent an email to Bob Stephan letting him know I had spoke with Sue but had not received the answers yet.
49. On Tuesday, October 23, 2007 at 7:03 pm I received an email which was addressed to Sue Armstrong from Bob Stephan. The emailed asked that I be forward the IP answers as soon as possible.
50. On Tuesday, October 23, 2007 at 7:06 pm I received an email from John Denning. The subject was Nomination Master Document. Attached were CS&C answers to the policy questions.

51. On Tuesday, October 23, 2007 at 7:07 pm I received an email from Bruce Landis thanking John Denning for sending the answers in.
52. On Tuesday, October 23, 2007 at 7:10 pm I received an email from Bob Stephan letting me know the answers had been sent.
53. On Tuesday, October 23, 2007 at 7:17 pm I received an email from Christopher Krebs clarifying and amending an answer regarding Infrastructure Protection's questions.
54. On Tuesday, October 23, 2007 at 7:18 pm I received an email from Greg Garcia acknowledging CS&C submission.
55. On Wednesday, October 24, 2007 at 12:30 pm I sent an email to Christopher Krebs and I CCed Sue Armstrong regarding a policy question that had not been answered.
    a. The this email exchange was in error as I never sent the question to them to begin with.
56. On Wednesday, October 24, 2007 at 12:32 pm I mailed Christopher Krebs and CCed Sue Armstrong looking for an answer to a policy question.
57. On Wednesday, October 24, 2007 at 12:34 pm I received an email from Sue Armstrong regarding a answer to a question regarding a policy question.
58. On Wednesday, October 24, 2007 at 12:35 I sent an email to Sue Armstrong and Christopher Krebs letting them know I was going back through all the questions to try to find the answer.
59. On Wednesday, October 24, 2007 at 12:37 pm I received an email from Sue Armstrong letting me know a question I had sent her was not in the original set of questions they had received.
60. On Wednesday, October 24, 2007 at 12:38 I sent an email to Sue Armstrong letting her know that I had only a partial answer to a question.
61. On Wednesday, October 24, 2007 at 12:43 pm I sent an email to Sue Armstrong with a CC to Christopher Krebs apologizing for the confusion; letting them know I had made a mistake and misread the question.
    a. This question that I could not find an answer to had never been sent to IP.
62. On Wednesday, October 24, 2007 at 1:10 pm I sent an email to Christopher Krebs and CCed Sue Armstrong. I thanked them for their assistance and let them know that Robert would be reviewing them.
63. On Wednesday, October 24, 2007 at 3:09 pm I sent an email to Matt Welbes at FTA/DOT asking him for assistance on getting the criteria for the War on Terrorism Medal.
64. On Wednesday, October 24, 2007 at 3:33pm I received an email from Christopher Krebs submitting a revised answer to question in IP's policy question section.
65. On Wednesday, October 24, 2007 at 4:18 pm I received an email from Matt Welbes referring me to Phyllis Soldo regarding the War on Terrorism Medal question.
66. On Wednesday, October 24, 2007 at 5:42 pm I sent an email to Kristina Dorville, David Hess, Jeanette Hanna-Ruiz and I CCed Robert Jamison on a draft of the policy questions.
    a. I pointed out that the first set of questions had yet to be completed and that I needed them to get me cleaned up responses by 10/25/07.

b. Sections II, III, and IV had not yet been completed at this point.

67. On Wednesday, October 24, 2007 at 6:16 pm I received an email from David Hess letting me know he was reviewing the draft answers I sent on 10/24/07 at 5:42 pm.
68. On Thursday, October 25, 2007 at 1:57 pm I received an email from David Hess recommending that we provide Robert the policy questions.
69. On Thursday, October 25, 2007 at 2:16 pm I received an email from Sue Armstrong letting me know that all the IP policy questions had been consolidated into one document for reference.
70. On Thursday, October 25, 2007 at 2:29 pm I sent an email to David Hess asking him for his comments and feedback.
71. On Thursday, October 25, 2007 at 2:35 pm I sent an email to Christopher Bonanti at FRA/DOT requesting assistance on the total number of FRA employees and budget while Robert was Acting Administrator.
72. On Thursday, October 25, 2007 at 2:36 pm I sent a note to Mark Kerksi and Mariana Merritt at TSA/DHS requesting the total budget number while Robert was Deputy Assistant Secretary.
73. On Thursday, October 25, 2007 at 2:42 pm I received an email from David Hess letting me know I would receive his edits soon.
74. On Thursday, October 25, 2007 at 3:29 pm I sent an email to Amanda Goodwin asking her is she was able to find the War on Terrorism criteria.
75. On Thursday, October 25, 2007 at 3:30 pm I received an email from David Hess letting me know that Kristin Royster would be sending me Office of Legislative Affairs (OLA) edits/comments.
76. On Thursday, October 25, 2007 at 3:30 pm I received an email from Amanda Goodwin regarding the status of the criteria for the War on terrorism medal.
77. On Thursday, October 25, 2007 at 3:47 pm I received an email from Kristin Royster with OLA edits and comments.
78. On Thursday, October 25, 2007 at 4:39 pm I received an email from Christopher Bonanti regarding the answer for the FRA question I had posed to him.
79. On Thursday, October 25, 2007 at 6:17 pm I sent an email to Robert Jamison with an attachment of questions for his review.
80. On Thursday, October 25, 2007 at 6:18 pm I sent an email to Robert Jamison with a copy of Julie Myers pre-hearing policy questions answered.
81. On Thursday, October 25, 2007 at 7:00 pm I sent an email to Robert Jamison and CCed Kristina Dorville, David Hess and Jeanette Hanna-Ruiz. The email contained the most current version of the policy questions.
    a. The emailed noted that this was not the final version and was not approved for dissemination. It also noted that Robert was still making changes.
82. On Thursday, October 25, 2007 at 7:15 pm from David Hess acknowledging receipt of the 10/25/07 7:00 pm email I had sent.
83. On Thursday, October 25, 2007 at 8:58 pm I forwarded the 10/25/07 7:00 pm email to Deborah Moore for review.
84. On Friday, October 26, 2007 at 8:46 am I received an email from David Hess letting me know he would be sending comments back by 9:30 am. This email

also reminded me that OGC (Office of the General Counsel) would need to review before being finalized.

85. On Friday, October 26, 2007 at 9:12 am I received an email from Robert Jamison with edits to the policy questions.
86. On Friday, October 26, 2007 at 9:36 am I sent an email to Kristina Dorville and CCed Helen Jackson. This email contained some of Robert's edits to questions.
    a. Helen Jackson is a contractor; however, she was not involved in the development of answers. She was CCed above to ensure that Kristina and the documents were printable in case for some reason Kristina had not received them.
    b. On 10/26/07 I had to hand off consolidation of editing to Kristina Dorville due to unexpected morning briefings for the Acting Deputy Secretary; Kristina Dorville had the pen on integrating all edits to the master document for the majority of the day.
87. On Friday, October 26, 2007 at 9:54 am I received an email from David Hess with his edits/comments to the policy questions.
88. On Friday, October 26, 2007 at 12:26 pm I received an email from Kristina Dorville. The attachment contained the policy questions with the consolidated edits.
89. On Friday, October 26, 2007 at 5:18 pm I received an email from Amanda Goodwin with information from DOT on the War on Terrorism Medal question.
    a. Amanda notes in her email that the information was given to her my Nancy Mowry, Dep Dir of HR at DOT.
90. On Friday, October 26, 2007 at 5:34 pm I sent an email to Robert Jamison with the latest version of the policy questions.
91. On Saturday, October 27, 2007 at 9:49 am I sent an email to Meghan Ludtke letting her know that Robert was editing all questions and was sending them to us for DHS review. I noted that the questions would be sent in batches.
92. On Saturday, October 27, 2007 at 9:53 am I sent an email to Meghan Ludtke clarifying my 10/27/07 9:49 am email.
93. On Saturday, October 27, 2007 at 10:37 am I received an email from Meghan Ludtke asking how many batches Robert would likely be sending.
94. On Saturday, October 27, 2007 at 1:22 pm I received an email from Robert Jamison with another review of the first 15 policy questions. This email was addressed to Meghan Ludtke, Jeanette Hanna-Ruiz, and David Hess.
    a. In this email he has highlighted areas that needed additional review.
95. On Saturday, October 27, 2007 at 1:31 pm I sent an email to Meghan Ludtke and David Hess requesting assistance on what the standard DHS answer for one of the questions.
96. On Saturday, October 27, 2007 at 2:32 I sent an email to Meghan Ludtke and David Hess asking for input on where there was a standard DHS for one of the policy questions.
97. On Saturday, October 27, 2007 at 2:36 pm I received an email in response to my email sent 10/27/07 at 2:32 pm from Meghan Ludtke. The email was addressed to Jeanette Hanna-Ruiz and David Hess with a CC to Joseph Maher.

a. In this email Meghan indicated that she will working with OGC/Leg to help get an answer to this question.

98. On Saturday, October 27, 2007 at 3:10 pm I received an email from Joseph Maher regarding getting assistance from the Mgmt Directorate on a policy question.
99. On Saturday, October 27, 2007 at 3:42 pm I received an email from David Hess. It was addressed to Robert Jamison, Jeanette Hanna-Ruiz, Meghan Ludtke and CCed were Kristina Dorville and Kristin Royster. The email contained edits/comments from David Hess to the first 15 questions.
100. On Saturday, October 27, 2007 at 3:45 pm I received an email from Robert Jamison. The email was addressed to David Hess, Meghan Ludtke, and Jeanette Hanna-Ruiz and CCed were Kristina Dorville and Kristin Royster. The email contained questions 16-26.
101. On Saturday, October 27, 2007 at 9:14 pm I received an email from David Hess. The email was addressed to Robert Jamison, Jeanette Hanna-Ruiz, Kristina Dorville, Kristin Royster, and Meghan Ludtke. It contained David's edits/comments to questions 16-26.
102. On Sunday, October 28, 2007 at 10:41 am I received an email from Meghan Ludtke who cleared for OGC questions 1-26. She noted additional coordination with DHS components was needed.
103. On Sunday, October 28, 2007 at 10:44 am I received an email from Robert Jamison with questions 27-37. This email was addressed to Meghan Ludtke, David Hess, Jeanette Hanna-Ruiz and CCed were Kristina Dorville and Kristin Royster.
104. On Sunday, October 28, 2007 at 11:05 am I received an email from Meghan Ludtke asking me if IP CSCD wrote the answers to the chem. questions.
105. On Sunday, October 28, 2007 at 11:19 am I received an email from Robert Jamison with questions 38-48. The email was addressed to Meghan Ludtke, David Hess, Jeanette Hanna-Ruiz and CCed were Kristina Dorville and Kristin Royster.
106. On Sunday, October 28, 2007 at 11:41 am I received an email from Robert Jamison addressed to me, Jeanette Hanna-Ruiz and CCed were Kristina Dorville, Kristin Royster, Meghan Ludtke, and David Hess. The email contained questions 49-57.
107. On Sunday, October 28, 2007 at 3:13 pm I received an email from Meghan Ludtke regarding edits to a chemical policy question.
108. On Sunday, October 28, 2007 at 6:05 pm I received an email from Meghan Ludtke regarding editing a sentence of one of the chemical questions.
109. On Sunday, October 28, 2007 at 6:19 pm I received an email from Meghan Ludtke regarding edits to questions 38-48. The email clarified this review did not constitute OGC clearance of this batch of questions.
110. On Sunday, October 28, 2007 at 9:21 pm I received an email from Meghan Ludtke regarding edits to a CS&C question.
111. On Sunday, October 28, 2007 at 9:38 pm I received an email from Meghan Ludtke regarding edits to questions 27-37.

112. On Sunday, October 28, 2007 at 9:56 I responded to Meghan Ludtke's email letting her know I had made the edit noted in her email sent on 10/28/07 at 9:35 pm.

113. On Sunday, October 28, 2007 at 10:12 pm I sent an email to Meghan Ludtke, David Hess, and Kristina Dorville with a CC to Robert Jamison and Kristin Royster. The email contained a consolidated version of the policy questions with all edits and comments.

   a. In this email I requested David Hess to help me identify standard language DHS had used in the past to answer questions.

114. On Monday, October 29, 2007 at 5:56 am I received an email from David Hess regarding consistency and Policy input. This emailed was addressed to Jeanette Hanna-Ruiz, Meghan Ludtke, and Kristina Dorville with a CC to Kristin Royster. This email noted that the questions needed to clear DHS and be sent to the Committee "today".

115. On Monday, October 29, 2007 at 6:28 am I received an email from David Hess; the email was addressed to Lee Morris.

   a. The email referenced my concern that the policy questions go through "appropriate final review before forwarding to the Committee."

116. On Monday, October 29, 2007 at 6:55 am I responded to the Hess email of 10/29/07 6:28 am noting that OGC did not clear all the questions over the weekend; that only 1-26 had been cleared by OGC over the weekend and the rest would need OGC clearance.

117. On Monday, October 29, 2007 at 7:39 am I sent an email to Don Kent and Gus Coldebella with a CC to David Hess, Meghan Ludtke, Lee Morris and Joseph Maher requesting assistance in obtaining full OGC and DHS clearance on the policy question answers.

118. On Monday, October 29, 2007 at 7:57 am I received an email from Lee Morris letting me know that OLA had the questions and would handle all the clearances.

119. On Monday, October 29, 2007 at 9:50 am I sent an email to Christopher Bonanti at FRA/DOT thanking him for his help.

120. On Monday, October 29, 2007 at 10:10 am I received an email from Meghan Ludtke addressed to Jeanette Hanna-Ruiz, Kristina Dorville and David Hess with a CC to Joseph Maher asking who had version control for additional edits.

121. On Monday, October 29, 2007 at 10:19 am I responded to Meghan's email of 10/29/07 10:10 am letting her know I would consolidate the edits.

122. On Monday, October 29, 2007 at 10:20 am I received an email from Lee Morris letting me know OLA would send questions for review but they needed a copy from NPPD for circulation.

123. On Monday, October 29, 2007 at 10:22 am I received an email from Meghan Ludtke on previous DHS answers to contractor related policy questions.

124. On Monday, October 29, 2007 at 10:23 am I sent an email to Lee Morris letting him know I would be sending him a clean copy of the policy questions.

125. On Monday, October 29, 2007 at 10:25 am I sent an email to Christopher Bonanti asking a question of how many FRA regional offices there were when Robert was Acting Administrator.
126. On Monday, October 29, 2007 at 10:26 am I received an email from Lee Morris regarding policy questions.
127. On Monday, October 29, 2007 at 10:30 am I received an email from Christopher Bonanti responding to my 10/29/07 10:25 am email.
128. On Monday, October 29, 2007 at 10:30 am I sent an email to Lee Morris indicating I would send David Hess a clean copy of the policy questions.
129. On Monday, October 29, 2007 at 10:48 am I received an email from Daniel Ahr that was addressed to Meghan Ludtke and CCed were Kristina Dorville and Jeanette Hanna-Ruiz adding edits to a CIIA question.
130. On Monday, October 29, 2007 at 10:53 am from Meghan Ludtke ensuring we had received Daniel Ahr's edits.
131. On Monday, October 29, 2007 at 11:02 am I received an email from Meghan Ludtke regarding adding language to a question.
132. On Monday, October 29, 2007 at 11:10 am I received an email from David Hess forwarding an email containing additional information that could used to answer a question related to contractors at DHS.
133. On Monday October 29, 2007 at 11:17 am I received an email from Meghan Ludtke forwarding me an email containing additional information that would be used to answer a question related to contractors at DHS.
134. On Monday, October 29, 2007 at 11:17 am I received an email from Scott Murphy addressed to David Hess, CCed are Jeanette Hanna-Ruiz, Christopher Richardson, Lee Morris, Nancy Friedman, Rosemary James, Randall Kaplan, Joseph Maher, Meghan Ludtke, and Kristina Dorville.
    a. The email noted that the answers were in "fairly good shape" and that ODC was still looking them over for further edits.
    b. The email also suggested DHS component agencies that would need to review particular questions.
135. On Monday, October 29, 2007 at 11:28 am I received an email from David Hess giving an update on status of policy question clearance. The email was addressed to Scott Murphy, Nancy Friedman, Randall Kaplan, and Meghan Ludtke with a CC to David Hess, Joseph Maher, Rosemary James, Christopher Richardson, Jeanette Hanna-Ruiz, Kristina Dorville, Lee Morris, Kristin Royster, and Timothy Johnson.
136. On Monday, October 29, 2007 at 11:44 am I sent an email to Deborah Moore asking her to remove the highlights and comments from the policy questions for DHS circulation.
137. On Monday, October 29, 2007 at 11:52 am I received an email from Meghan Ludtke addressed to David Hess, Scott Murphy, Nancy Friedman, Randall Kaplan, Meghan Ludtke with a CC to Joseph Maher, Rosemary James, Christopher Richardson, Jeanette Hanna-Ruiz, Kristina Dorville, Lee Morris, Kristin Royster and Timothy Johnson.
    a. This email notes the importance of ensuring DHS component review when they have equities in the answer to the question.

138. On Monday, October 28, 2007 at 12:08 pm I received an email from Deborah Moore with the policy questions attached.
139. On Monday, October 29, 2007 at 12:29 pm I received an email from David Hess addressed to Meghan Ludtke and Scott Murphy with a CC to Joseph Maher, Kristin Royster, Jeanette Hanna-Ruiz, Kristina Dorville and Lee Morris noting the time constraints and discussing the clearance process.
140. On Monday, October 29, 2007 at 12:56 pm I sent Lee Morris and David Hess a clean copy of the policy questions.
141. On Monday, October 29, 2007 at 12:56 pm I received an email from Lee Morris acknowledging receipt of a clean copy of the policy questions for DHS clearance.
142. On Monday, October 29, 2007 at 1:14 pm I received an email from David Hess addressed to me and Lee Morris. The emailed noted that clearance should be handled through NPPD Exec Sec in addition to noting OGC's suggested DHS clearance offices.
143. On Monday, October 29, 2007 at 1:15 I responded to David's 10/29/07 1:14 pm email stating that we needed to include the list of components I had developed for review of policy questions.
144. On Monday, October 29, 2007 at 1:15 pm I received an email from Lee Morris concurring with the email sent by David Hess on 10/29/07 at 1:14pm.
145. On Monday, October 29, 2007 at 1:21 pm I sent an email to Deborah Moore with one DHS component distribution list.
146. On Monday, October 29, 2007 at 1:21 pm I sent Deborah Moore an email containing a second set of DHS components for review of policy questions.
147. On Monday, October 29, 2007 at 1:23 pm I sent an email to Meghan Ludtke and CCed David Hess and Deborah Moore; this email asked that Leg or OGC task the review to get timely responses back.
148. On Monday, October 29, 2007 at 1:40 pm I received an email from David Hess regarding clearance of questions through components.
149. On Monday, October 29, 2007 at 1:45 pm I sent an email to Scott Murphy with a clean copy of the policy questions asking him to send edits back to Deborah Moore with a CC to Kristina Dorville and me for adjudication.
150. On Monday, October 29, 2007 at 1:46 pm I sent a clean copy of the policy questions to Scott Murphy.
151. On Monday, October 29, 2007 at 3:05 pm I received an email from Nancy Friedman addressed to Deborah Moore; CCed were Kristina Dorville, Jeanette Hanna-Ruiz, Lee Morris, David Hess, Scott Murphy, and Meghan Ludtke. The email noted U.S. Coast Guard concurred on question #28.
152. On Monday, October 29, 2007 at 3:06 pm I received an email from Deborah Moore that was addressed to Nancy Friedman with a CC to Kristina Dorville, Jeanette Hanna-Ruiz, Lee Morris, David Hess, Scott Murphy, and Meghan Ludtke. Deborah acknowledges receipt of Nancy's 10/29/07 3:05 pm email.
153. On Monday, October 29, 2007 at 3:41 pm I received an email from Nancy Friedman addressed to Deborah Moore with a CC to Kristina Dorville, Jeanette Hanna-Ruiz, Lee Morris, David Hess, Scott Murphy and Meghan Ludtke noting

that the DHS Office of Science and Technology had cleared questions 45, 47, and 48 with no comments.

154. On Monday, October 29, 2007 at 4:36 pm I sent an email to Deborah Moore regarding consistency of answers.

155. On Monday, October 29, 2007 at 4:44 pm I received an email from Deborah Moore regarding consistency.

156. On Monday, October 29, 2007 at 5:00 pm I received an email from Deborah Moore that was addressed to Nancy Friedman with a CC to Kristina Dorville, Jeanette Hanna-Ruiz, Lee Morris, David Hess, Scott Murphy, and Meghan Ludtke regarding status of clearance in the components.

157. On Monday, October 29, 2007 at 5:07 pm I received an email from Scott Murphy addressed to Nancy Friedman and Deborah Moore and CCed to Kristina Dorville, Jeanette Hanna-Ruiz, Lee Morris, David Hess, and Meghan Ludtke regarding the status of clearance of questions in the components.

158. On Monday, October 29, 2007 at 5:24 pm I received an email from Deborah Moore addressed to Jacalynne Becker and CCed to Elizabeth Gary and Jeanette Hanna-Ruiz requesting the CoS list for DHS to double check our written responses.

159. On Monday, October 29, 2007 at 5:28 pm I received an email from David Hess addressed to Scott Murphy, Deborah Moore and Nancy Friedman and CCed to Kristina Dorville, Jeanette Hanna-Ruiz, Lee Morris and Meghan Ludtke letting us know that the Committee needed the questions and we had until noon 10/30/07 to deliver the questions.

160. On Monday, October 29, 2007 at 5:29 pm I received an email from Jacalynne Becker addressed to Deborah Moore responding to Deborah's 10/29/07 5:24 pm email.

161. On Monday, October 29, 2007 at 5:30 pm I received an email from Deborah Moore regarding edits question #41.

162. On Monday, October 29, 2007 at 5:31 pm I sent an email to Deborah Moore regarding question #41 directing them to ensure Robert was OK with edit "since he wrote them."

163. On Monday, October 29, 2007 at 5:31 pm I received an email from Deborah Moore acknowledging that we needed Robert's input on question #41 in light of the edits.

164. On Monday, October 29, 2007 at 5:31 pm I sent an email to Deborah Moore ensuring we had SCO, ICE and CBP review.

165. On Monday, October 29, 2007 at 5:33 pm I received an email from Deborah Moore regarding my concern that SCO, ICE and CBP needed to review the US-VISIT answers to the policy questions.

166. On Monday, October 29, 2007 at 5:36 pm I received an email from Nancy Friedman regarding component comments.

167. On Monday, October 29, 2007 at 5:43 pm I received an email from Deborah Moore regarding U.S. Secret Service edits/comments to question #34.

168. On Monday, October 29, 2007 at 5:47 pm I received an email from David Hess requesting we finalize comments to give to Robert for final review.

169. On Monday, October 29,2 007 at 5:48 I sent an edit to Deborah Moore regarding PSAs and the U.S. Secret Service (USSS).
170. On Monday, October 29, 2007 at 5:49 pm I sent an email to Deborah Moore and Kristina Dorville about way forward with policy questions.
171. On Monday, October 29, 2007 at 5:58 pm I received an email from Deborah Moore regarding Federal Emergency Management Administration (FEMA) comments to an IP question regarding PSAs.
172. On Monday, October 29, 2007 at 6:04 pm I received an email from Deborah Moore addressed to Brian White and CCed to Jeanette Hanna-Ruiz, Elizabeth Gary, Kristina Dorville, and Kathleen Kraninger regarding Policy and SCO input on questions 51, 52, 53, and 54.
173. On Monday, October 29, 2007 at 6:19 pm I received an email from Deborah Moore addressed to Kathleen Montgomery and CCed to Jeanette Hanna-Ruiz and Elizabeth Gary regarding Office of Public Affairs input on questions 46, 47, and 48.
174. On Monday, October 29, 2007 at 6:21 pm I received an email from Deborah Moore addressed to Steve Atrkiss and CCed to Jeanette Hanna-Ruiz and Elizabeth Gary regarding Customs and Border Patrol input on questions 51, 52, 53, and 54.
175. On Monday, October 29, 2007 at 6:26 pm I received an email from Deborah Moore addressed to David Hess requesting assistance from OLA on questions 11 and 29.
176. On Monday, October 29, 2007 at 6:27 pm I received an email from Kathleen Kraninger addressed to Brian White, Deborah Moore and Jeanette Hanna-Ruiz with a CC to Richele Cole that contained edits to questions 51c and 53.
177. On Monday, October 29, 2007 at 6:31 pm I received an email from Deborah Moore addressed to Thad Bingel with a CC to Elizabeth Gary and Jeanette Hanna-Ruiz regarding input from Custom and Border Patrol to questions 51, 52, 53, 54, and 34
178. On Monday, October 29, 2007 at 6:31 pm I received an email from Elizabeth Gary addressed to Deborah Moore, Jeanette Hanna-Ruiz, and Kristina Dorville regarding FEMA comments.
179. On Monday, October 29, 2007 at 6:33 pm I received an email from David Hess addressed to Deborah Moore and CCed to Kristin Royster, Elizabeth Gary, Jeanette Hanna-Ruiz, Lee Morris, and Kristina Dorville responding Deborah's 10/29/07 6:26 pm email.
180. On Monday, October 29, 2007 at 6:41 pm I received an email from Deborah Moore addressed to Jordan Gottfried and CCed to Jeanette Hanna-Ruiz and Elizabeth Gary regarding input on a question regarding CI/KR and incidents.
181. On Monday, October 29, 2007 at 6:58 pm I received an email from Jordan Gottfried responding to Deborah's 10/29/07 6:33 pm email.
182. On Monday October 29, 2007 at 7:00 pm I received an email from Deborah Moore regarding edits to the question regarding PSAs.
183. On Monday, October 29, 2007 at 7:00 pm I sent an email to Deborah Moore agreeing with her reword of the PSA and USSS sentence.

184. On Monday, October 29, 2007 at 7:08 pm I sent email to Deborah Moore asking is we sent the questions to TSA and the Management Directorate for input.
185. On Monday, October 29, 2007 at 7:09 pm I received an email from Deborah Moore confirming that we received Management Directorate and Transportation Security Administration input.
186. On Monday, October 29, 2007 at 7:22 pm I received an email from Deborah Moore to Jessica Reyes regarding contractors and full time employees in the Office of Infrastructure Protection (OIP).
187. On Monday, October 29, 2007 at 7:40 I sent an email to Deborah Moore and Jessica Reyes with a CC to Elizabeth Gary regarding Deborah's 10/29/07 7:22 pm email to Jessica Reyes.
188. On Monday, October 29, 2007 at 7:56 pm I received an email from Deborah Moore addressed to Robert Jamison and CC to me. The email contained the policy questions with component input.
189. On Monday, October 29, 2007 at 7:57 pm I received an email from Jessica Reyes addressed to Deborah Moore and myself with a CC to Elizabeth Gary responding to Deborah's 10/29/07 7:22 pm email regarding contractor-full time employee ration in the OIP.
190. On Monday, October 29, 2007 at 8:00 pm I received an email from Kristina Dorville addressed to Allison Boyd and CCed to Jeanette Hanna-Ruiz, Deborah Moore and Elizabeth Gary requesting her input on questions 16, 17, 29, 30, and 31.
191. On Monday, October 29, 2007 at 8:59 pm I received an email from Allison Boyd responding and providing edits/comments to Kristina's 10/29/07 8:00 pm email.
192. On Monday, October 29, 2007 at 9:05 pm I received an email from Kathleen Montgomery addressed to Deborah Moore and CCed to Elizabeth Gary and me requesting the questions be resent in response to Deborah's 10/29/07 6:19 pm email.
193. On Tuesday, October 30, 2007 at 7:57 am I received an email from David Hess addressed to Deborah Moore; CCed to Meghan Ludtke, Kristina Dorville, Jeanette Hanna-Ruiz, and Lee Morris with edits to question 29.
194. On Tuesday, October 30, 2007 at 7:58 am I received an email from Deborah Moore responding to David's 10/30/07 7:57 am email acknowledging edits.
195. On Tuesday, October 30, 1007 at 8:04 am I received an email from Meghan Ludtke addressed to David Hess and Deborah Moore with a CC to Kristina Dorville, Jeanette Hanna-Ruiz, and Lee Morris concurring with edits to question 29.
196. On Tuesday, October 30, 2007 at 9:17 am I received an email from Deborah Moore with the latest consolidated policy questions.
197. On Tuesday, October 30, 2007 at 9:23 pm I received an email from Deborah Moore regarding who at CBP was reviewing the questions.
198. On Tuesday, October 30, 2007 at 9:34 am I received an email addressed to Meghan Ludtke discussing comments from Allison Boyd over chemical security answers.

199. On Tuesday, October 30, 2007 at 9:53 am I received an email from Meghan Ludtke addressed to Deborah Moore discussing the 10/30/07 9:34 am email.
200. On Tuesday, October 30, 2007 at 10:12 am I sent an email to Deborah asking who we were sending to at CBP.
201. On Tuesday, October 30, 2007 at 10:12 I received an email from Deborah Moore noting that questions for CBP were sent to Thad Bingel.
202. On Tuesday, October 30, 2007 at 10:13 am I sent an email to Deborah Moore acknowledging receipt of her CBP POC.
203. On Tuesday, October 30, 2007 at 11:50 am I sent an email to Deborah Moore asking her if she got edits to question 28b.
204. On Tuesday, October 30, 2007 at 11:50 am I sent an email to Deborah Moore asking her if she got edits to question 27.
205. On Tuesday, October 30, 2007 at 11:50 am I sent an email to Deborah Moore asking her if she got edits to question 27.
206. On Tuesday, October 30, 2007 at 11:53 am I received an email from Deborah Moore regarding edits to questions 27 and 28.
207. On Tuesday, October 30, 2007 at 11:58 am I received an email from Deborah Moore recapping status of questions.
    a. In this email she notes that "Mr. Jamison last night reviewed what we had…"
208. On Tuesday, October 30, 2007 at 11:58 I sent an email to Deborah Moore requesting the latest version of the policy questions.
209. On Tuesday, October 30, 2007 at 11:59 am I received an email from Deborah wit he latest draft of the policy questions.
210. On Tuesday, October 30, 2007 at 12:13 pm I received an email from Deborah Moore addressed to Meghan Ludtke regarding the edits to a chemical question.
211. On Tuesday, October 30, 2007 at 12:15 I received an email from Deborah Moore regarding Office of Public Affairs (OPA) input.
212. On Tuesday, October 30, 2007 at 12:40 pm I received an email from David Hess responding to Deborah's 10/30/07 12:15 pm email regarding OPA input.
213. On Tuesday, October 30, 2007 at 12:25 pm I sent an email to Deborah Moore responding to her 10/30/07 12:15 pm.
214. On Tuesday, October 30, 2007 at 12:50 pm I sent an email to Meghan Ludtke asking if we could get the notary on standby for 2 hours.
215. On Tuesday, October 30, 2007 at 12:50 pm I received an email from Meghan Ludtke regarding the notary.
216. On Tuesday, October 30, 1007 at 12:51 pm I sent an email to Meghan Ludtke clarifying need of a notary.
217. On Tuesday, October 30, 2007 at 12:55 pm I received an email from Meghan Ludtke regarding the notary.
218. On Tuesday, October 30, 2007 at 1:05 pm I received an email from David Hess addressed to Timothy Johnson and Erin White with a CC to Lee Morris and me regarding getting notarized policy questions to Committee.

219. On Tuesday, October 30, 2007 at 1:24 pm I received an email from David Hess addressed to Erin White, Timothy Johnson and CC to Lee Morris and me regarding POC at the Committee.
220. On Tuesday, October 30, 2007 at 1:26 pm I received an email from Erin White responding to David's 10/30/07 1:05 pm email acknowledging she could take documents to Committee.
221. On Tuesday, October 30, 2007 at 1:35 pm I received an email from Timothy Johnson regarding his availability to assist in getting questions to Committee.
222. On Tuesday, October 30, 2007 at 2:19 pm I received an email from Deborah Moore addressed to Erin Street and CCed are David Hess and me regarding OPA input.
223. On Tuesday, October 30, 2007 at 2:37 pm I received an email from Charlie Payne regarding a question on the Office of Bombing Prevention.
224. On Tuesday, October 30, 2007 at 2:39 pm I received an email from William Flynn regarding a question on the Office of Bombing Prevention.
225. On Tuesday, October 30, 2007 at 2:42 pm I received an email from Deborah Moore with the latest policy questions consolidated.
226. On Tuesday, October 30, 2007 at 2:44 pm I received an email from Mary Ann Woodson regarding a question on the Office of Bombing Prevention.
227. On Tuesday, October 30, 2007 at 3:37 pm I received an email from Deborah Moore regarding edits to the chemical security questions.
228. On Tuesday, October 30, 2007 at 3:58 pm I received an email from Deborah Moore with the consolidated questions and edits.
229. On Tuesday, October 30, 2007 at 4:35 pm I sent an email to David Hess regarding status of the policy questions.
230. On Tuesday, October 30, 2007 at 4:37 pm I received an email from David Hess regarding edits to questions.
231. On Tuesday, October 30, 2007 at 4:52 pm I received an email from Allison Boyd regarding edits to the chemical security question.
232. On Tuesday, October 30, 2007 at 5:01 pm I sent an email to Allison Boyd acknowledging her edits to the chemical questions.
233. On Tuesday, October 30, 2007 at 5:04 pm I received an email from Deborah Moore with edits to the chemical security questions.
234. On Tuesday, October 30, 2007 at 5:10 pm sent an email to Robert Jamison letting him know we were working on the questions as edits were still coming through.
235. On Tuesday, October 30, 2007 at 6:11 pm I received an email from Elizabeth Gary CCed were Coleman Mehta, Deborah Moore, and Elizabeth Gary; the email contained a PDF of the final policy questions.
236. On Tuesday, October 30, 2007 at 6:11 pm I sent an email to David Hess, Lee Morris and CCed Robert Jamison with the final policy questions.
237. On Tuesday, October 30, 2007 at 6:12 pm I received an email from Lee Morris confirming receipt of the final policy questions.
238. On Wednesday, October 31, 2007 at 9:35 am I received an email from Kristina Dorville looking for the original policy questions.

239. On Wednesday, October 31, 2007 at 9:36 am I sent an email to Kristina Dorville acknowledging I had the original policy questions.
240. On Wednesday, October 31, 2007 at 9:43 am I received an email from Kristina Dorville letting me know that the original documents needed to be delivered to the Committee.
241. On Wednesday, October 31, 3007 at 9:47 am I received an email from Deborah Moore with additional OGC edits.
242. On Tuesday, November 6, 2007 at 5:14 pm I received an email from David Hess addressed to me, Lee Morris, and Robert Jamison with a CC to Kristin Royster and Kristina Dorville regarding additional pre-hearing questions for Robert.
243. On Wednesday, November 7, 2007 at approximately 9:40 I met with Robert Mocny, Bob Stephan, Anne Petera, Tina Gabbrielli in NAC building 20 and Hun Kim was present via secure video teleconference. Also present in the room was Kristina Dorville.
    a. At this time reminded each person of the original direction given with the first set of questions that they only be answered by SES level and above officials. Everyone present acknowledged that direction.
    b. I let the parties present know that during Robert's staff interview went well and I thanked them for their support.
    c. I then discussed the next set of policy questions that had arrived. That the questions (1 and 2) dealt specifically with contractor involvement in answering the questions.
    d. I told them we did not care if the answer was yes or not but we wanted to know the accurate answer to be able to answer truthfully.
    e. During the meeting, Tina Gabbrielli handed me a note stating no contractors were used in answering RMA questions.
    f. Robert Mocny pointed out that he had no SES level folks but that senior level (GS-15 level folks) had answered the questions.
    g. Each direct report to Robert was tasked with getting back to me by COB with an answer.
244. On Wednesday, November 7, 2007 at 12:48 pm I received an email from David Hess addressed to Kristina Dorville and I with a CC to Kristin Royster and Helen Jackson regarding status of the additional questions.
245. On Wednesday, November 7, 2007 at 1:37 pm I received an email from Greg Garcia asking for clarification on the additional policy questions.
246. On Wednesday, November 7, 2007 at 1:38 pm I received an email from Hun Kim regarding CS&Cs answer on contractor use.
247. On Wednesday, November 7, 2007 at 4:10 pm I received an email from Robert Mocny regarding US-VISIT answer on contractor use.
248. On Wednesday, November 7, 2007 in the later part of the afternoon Bob Stephan came by my office to tell me IP did not use contractors to answer questions.
    a. Sue Armstrong had called me earlier to let me know this as well.

249. On Wednesday, November 7, 2007 at 6:55 pm I sent an email to Gus Coldebella and Julie Dunne. The email contained the additional pre-hearing questions.
250. On Thursday, November 8, 2007 in the morning I had two conference calls regarding if contractors were used to answer any of the questions.
    a. The first call was with Julie Dunne and Greg Garcia.
    b. The second call was with Julie Dunne and Cheri McGuire.
251. On Thursday, November 8, 2007 at 11:26 am I sent an email to Julie Dunne regarding the additional pre-hearing policy questions.
252. On Thursday, November 8, 2007 at 11:43 am I sent an email to Cheri McGuire regarding NCSD answers that were submitted to the Committee.
253. On Thursday, November 8, 2007 at 11:58 am I sent an email to Julie Dunne regarding questions 44, 45, 47, 48, and 49 based on a conversation I had with Cheri McGuire.
254. On Thursday, November 8, 2007 at 12:11 pm I received an email from Julie Dunn regarding draft answers to the additional policy questions.
255. On Thursday, November 8, 2007 at 1:!6 pm I sent Robert Jamison and CCed Kristina Dorville on an email containing draft responses to the additional two pre-hearing policy questions.
256. On Thursday, November 8, 2007 at 1:17 pm I sent an email to Robert D Jamison regarding possible answer to the additional two policy questions.
257. On Thursday, November 8, 2007 sometime between 1:00 – 2:00 pm I spoke with Robert Jamison regarding his edits to the answers.
258. On Thursday, November 8, 2007 at 1:30 pm I received an email from Kristina Dorville with Robert's edits to the additional policy question answers.
259. On Thursday, November 8, 2007 at 1:52 pm I sent an email to Julie Dunne and Gus Coldebella regarding Robert's revisions to the draft answers.
260. On Thursday, November 8, 2007 at 1:54 pm I sent an email to Meghan Ludtke regarding need for a notary.
261. On Thursday, November 8, 2007 ay 1:58 pm I received an email Meghan Ludtke regarding the status of the notary.
262. On Thursday, November 8, 2007 at 2:02 pm I sent an email to Meghan Ludtke regarding need of a notary.
263. On Thursday, November 8, 2007 at 2:03 pm I sent an email to Julie Dunne regarding clearance from Gus on the answers.
264. On Thursday, November 8, 2007 at 2:45 pm I sent an email to Julie Dunne regarding clearance from Gus.
265. On Thursday, November 8, 2007 at 2:54 pm I sent an email to Meghan Ludtke on status of notary.
266. On Thursday, November 8, 2007 at 2:54 pm I received an email from Meghan Ludtke regarding the notary.
267. On Thursday, November 8, 2007 at 2:55 pm I sent an email to Meghan Ludtke regarding the additional questions and the notary.
268. On Thursday, November 8, 2007 at 3:00 pm I emailed Julie Dunne regarding edits from Gus.

269. On Thursday, November 8, 2007 ay 3:02 pm I emailed Meghan Ludtke on notary issue.
270. On Thursday, November 8, 2007 at 3:01 pm I received an email from Meghan Ludtke regarding the notary.
271. On Thursday, November 8, 2007 at 3:06 pm I emailed David Hess on status of the additional questions.
272. On Thursday, November 8, 2007 at 3:08 pm I received an email from David Hess regarding the status of the responses to the additional questions.
273. On Thursday, November 8, 2007 at 3:10 pm I received an email from David Hess regarding the status of the responses to the additional questions.
274. On Friday, November 9, 2007 between 5:00 – 6:00 pm I spoke with Robert Jamison regarding the use of contractors in answering policy questions.
275. On Friday, November 9, 2007 after 6:00 pm the following events transpired:
    a. I had a discussion with David Hess.
    b. I had a conference call with Gus Coldebella, David Hess, Lee Morris, and Robert Jamison
    c. I had another discussion with David Hess.
    d. Throughout the night I spoke to Robert Jamison.
    e. At ~9:00 pm I had a conference call with Gus Coldebella and David Hess.
    f. At ~9:30 pm David Hess and I spoke via conference call to Robert Jamison.
    g. At 10:15 pm I convened a conference call of: David Hess, Tina Gabbrielli, Greg Garcia, Bob Stephan, and Robert Mocny. Mr Stephan was not able to join the call so I spoke to him separately with David Hess on that call.
        i. The purpose of the 10:15 pm call was to let the senior leadership that we had additional questions arrive that would need to be answered and in particular to draw their attention to question #6.
        ii. I reminded them of the original guidance that only SES level and above were directed to answer questions; and that Robert had signed a statement based on their responses to me that the only contractor input may have been in NCSD.
        iii. They all reiterated that their statements that no contractors were involved and agreed to go back over the weekend and do a rescrub of all questions.
        iv. We agreed that all questions going forward would only be answered by the senior management team: Greg Garcia, Bob Stephan, Robert Mocny, Tina Gabbrielli, myself and Robert Jamison.
276. On Friday, November 9, 2007 at 7:16 pm I received an email from David Hess containing the follow up Lieberman QFRs.
277. On Friday, November 9, 2007 at 10:27 pm I received an email from Robert Mocny asking me what our conference call was about.
278. On Saturday, November 10, 2007 at 7:34 am I received an email from David Hess that contained Akaka QFRs.

279. On Friday, November 9, 2007 at 8:26pm I sent an email to David Hess and Gus Coldebella regarding a conference call on the additional questions.
280. On Friday, November 9, 2007 at 9:37 pm I sent Robert Jamison the conference call line information.
281. On Friday, November 9, 2007 at 10:01 pm I sent an email to Greg Garcia, Bob Stephan, Tina Gabbrielli, and Robert Mocny regarding a conference call.
282. On Friday, November 9, 2007 at 10:19 pm I sent an email to Bob Stephan and Richard Driggers trying to locate Bob Stephan.
283. On Friday, November 9, 2007 at 10:53 pm I sent an email to Bob Stephan, Greg Garcia, Tina Gabbrielli, and Robert Mocny with a CC to David Hess regarding question #6 and that this rescrub should only be done by SES level and above.
284. On Saturday, November 10, 2007 at 8:59 am I received am email from Greg Garcia asking for the deadline for the latest tasking.
285. On Saturday, November 10, 2007 at 9:13 am I sent an email to Greg Garcia, Bob Stephan, Tina Gabbrielli, and Robert Mocny with a CC to David Hess regarding the timeline to have the rescrub done.
286. On Saturday, November 10, 2007 at 9:24 am I sent an email to David Hess regarding the way forward with the additional questions.
287. On Saturday, November 10, 2007 at 9:40 am I received am email from Greg Garcia letting me know Cheri McGuire would be doing the scrub for NCSD.
288. On Saturday, November 10, 2007 at 11:48 am I received an email from Sue Armstrong documenting who answered IPs policy questions.
    a. She notes that IP answers were developed by federal employees only.
289. On Saturday, November 10, 2007 at 11:49 am I sent an email to Sue Armstrong acknowledging her email of 11/10/07 11:48 am.
290. On Saturday, November 10, 2007 at 2:45 pm I received an email form Sue Armstrong documenting how IP answered each question who which full time government employees participated in this task.
291. On Saturday, November 10, 2007 at 2:49 pm I sent an email to Sue Armstrong and Bob Stephan acknowledging receipt of their additional information.
292. On Saturday, November 10, 2007 at 4:00 pm I received an email from Tina Gabbrielli stating that no contractors were used in developing RMAs answers.
293. On Saturday, November 10, 2007 at 4:03 pm I sent an email to Tina Gabbrielli acknowledging receipt of her 11/10/07 4:00 pm email.
294. On Saturday, November 10, 2007 at 11:39 pm I sent an email to Greg Garcia letting him know I had not yet received CS&C input.
295. On Saturday, November 10, 2007 at 11:43 pm I sent an email to Robert Mocny letting him know I had not yet received US-VISIT input.
296. On Saturday, November 10, 2007 at 11:43 pm I forwarded my 11/10/07 11:43 pm email to Penelope Smith.
297. On Saturday, November 10, 2007 at 11:45 pm I forwarded my 11/10/07 11:39 pm email to Hun Kim and Cheri McGuire.

298. On Saturday, November 10, 2007 at 11:45 pm I sent an update to David Hess and CCed Robert Jamison.
299. On Sunday November 11, 2007 at 1:04 am I received an email from Cheri McGuire letting me know she would be completing the scrub.
300. On Sunday, November 11, 2007 at 9:11 am I received an email from Robert Mocny acknowledging Penelope Smith was doing the rescrub for US-VISIT.
301. On Sunday, November 11, 2007 at 2:58 pm I received an email from Cheri McGuire regarding the status of the rescrub for NCSD.
    a. This email contained an attachment answering question #6 from Sen. Lieberman.
302. On Sunday, November 11, 2007 at 3:50 pm I sent an email to Greg Garcia, Hun Kim and Cheri McGuire thanking them for their assistance and asking for confirmation that a rescrub had found no contractors answered questions in OEC and NCS.
303. On Sunday, November 11, 2007 at 4:24 pm I received an email from Hun Kim addressed to me, Greg Garcia and Cheri McGuire stating that OEC, NCCC, and NCS confirm that they did not use contractors.
304. On Sunday, November 11, 2007 at 4:44 pm I sent an email to David Hess, Gus Coldebella and Robert Jamison regarding a timeline of events for the pre- and post-hearing policy questions.
305. On Sunday, November 11, 2007 at 4:53 pm I sent an email to David Hess, Gus Coldebella and Robert Jamison confirming that no contractors were involved with the answering of pre-hearing policy questions that remained in OUS.
306. On Sunday, November 11, 2007 at 5:23 pm I received an email from Penelope Smith addressed to Robert Mocny and me stating that all answers to pre-hearing policy questions were addressed and written by GS-15 staff.
307. On Sunday, November 11, 2007 at 5:25 pm I sent an email to Penelope Smith acknowledging her 10/11/07 5:23 email.
308. On Sunday, November 11, 2007 at 11:05 pm I sent an email to Robert Mocny regarding draft answers to the post-hearing questions.
309. On Sunday, November 11, 2007 at 11:10 pm I sent an email to Bob Stephan regarding draft answers to the post-hearing questions.
310. On Sunday, November 11, 2007 at 11:11 pm I sent an email to Tina Gabbrielli regarding draft answers to the post-hearing questions.
311. On Sunday, November 11, 2007 at 11:14 pm I sent an email to Mary Ann Woodson regarding draft answers to the post-hearing questions.
312. On Sunday, November 11, 2007 at 11:19 pm I sent an email to Elizabeth Gary regarding draft answers to the post-hearing questions.
313. On Sunday, November 11, 2007 at 11:19 pm I sent an email to Robert Jamison regarding draft answers to the post-hearing questions.
314. On Sunday, November 11, 2007 at 11:19 pm I sent an email to Elizabeth Gary regarding the Employee Advisory Council post-haring question.
315. Sunday, November 11, 2007 at 11:22 pm I received an email from Elizabeth Gary confirming that there was only one question.

316. On Sunday, November 11, 2007 at 11:23 pm I sent an email to Mary Ann Woodson requesting assistance on a post-hearing follow up question.
317. On Sunday, November 11, 2007 at 11:23 pm I sent an email to Robert Jamison requesting input on post-hearing policy questions.
318. On Sunday, November 11, 2007 at 11:24 pm I sent an email to David Hess and Lee Morris regarding the status of the post-hearing questions.
319. On Monday, November 12, 1007 at 7:52 am I received an email from Tina Gabbrielli confirming she received the draft answers to the post-hearing policy questions; and would review and edit them.
320. On Monday, November 12, 2007 at 10:50 am I sent an email to Manny Rodriguez regarding the post-hearing questions.
321. On Monday, November 12, 2007 at 10:52 am I sent an email to Sue Armstrong asking the status of the IP post-hearing follow up questions.
322. On Monday, November 12, 2007 at 10:53 I sent an email to Penelope Smith regarding status of the post-hearing questions for US-VISIT.
323. On Monday, November 12, 2007 at 11:08 am I received an email from Sue Armstrong letting me know that she would follow up with Bob Stephan.
324. On Monday, November 12, 2007 at 12:47 pm I received an email from Robert Mocny confirming I would have US-VISIT review and edits by COB.
325. On Monday, November 12, 2007 at 2:15 pm I received an email from Tina Gabbrielli with her edits to the post-hearing follow up questions.
326. On Monday, November 12, 2007 at 2:35 pm I received an email from Penelope Smith letting me know that Robert Mocny was engaged in reviewing the post-hearing policy questions.
327. On Monday, November 12, 2007 at 2:49 pm I received an email from Robert Mocny with his review and edits to the US-VISIT post-hearing policy questions.
328. On Monday, November 12, 2007 at 2:58 pm I sent an email to Robert Mocny acknowledging his 10/12/07 2:49 pm email.
329. On Monday, November 12, 2007 at 4:26 pm I received an email from Cheri McGuire regarding NCSD/CS&C edits and review of the post-hearing follow up questions.
330. On Monday, November 12, 2007 at 5:16 pm I received an email from Manny Rodriguez regarding a post-hearing follow up question.
331. On Monday, November 12, 2007 at 6:03 pm I sent an email to Manny Rodriguez regarding the post- hearing follow up questions.
332. On Monday, November 12, 2007 at 6:17 pm I received a follow up email from Manny Rodriguez.
333. On Monday, November 12, 2007 at 6:31 pm I received an email from Bob Stephan letting me know he was working the IP post-hearing questions.
334. On Monday, November 12, 2007 at 6:56 pm I sent an email to Robert Jamison and David Hess regarding status of all hearing question activities.
335. On Monday, November 12, 2007 at 7:00 pm I sent an email to Robert Jamison and CCed David Hess with a status of the post-hearing follow up questions.
    a. Though the email states there is an attachment, I forgot to attach it.

336. On Monday, November 12, 2007 at 8:02 pm I received an email from Elizabeth Gary responding to a post-hearing policy question.
337. On Tuesday, November 13, 2007 at 7:40 am I received an email from Manny Rodriguez that the post-hearing follow up questions was being worked on.
338. On Monday, November 13, 2007 at 8:18 am I received an email from Manny Rodriguez following up on the post-hearing policy question he is helping answer.
339. On Tuesday, November 13, 2007 at 3:44 am I sent Bob Stephan an email regarding the status of the hearing questions.
340. On Tuesday, November 13, 2007 at 3:46 am I sent an email to Manny Rodriguez regarding post-hearing questions.
341. On Tuesday, November 13, 2007 at 7:41 am I sent an email to Manny Rodriguez regarding post-hearing questions.
342. On Tuesday, November 13, 2007 at 7:42 am I sent an email to Manny Rodriguez regarding post-hearing questions.
343. On Tuesday, November 13, 2007 at 8:52 am I received an email from David Hess regarding the status of the post-hearing follow up questions.
344. On Tuesday, November 13, 2007 at 9:22 am I sent an email responding to David's 11/13/07 8:52 am email.
345. On Tuesday, November 13, 2007 at 10:02 am I sent an email to Bob Stephan and Sue Armstrong regarding the status of the post-hearing follow up questions.
346. On Tuesday, November 13, 2007 at 10:57 am I received an email from Sue Armstrong regarding IPs post-hearing questions.
347. On Tuesday, November 13, 2007 at 11:20 am I received an email from Lawrence Stanton of IP on IPs post-hearing questions.

Senator Daniel K. Akaka
Additional Questions for the Record
Nomination Hearing of Robert D. Jamison
November 9, 2007

1. There is concern that the new Office of Bombing Prevention (OBP) may duplicate existing functions that already exist within the Departments of Defense and Justice regarding IEDs. The Bureau of Alcohol, Tobacco and Firearms has its U.S. Bomb Data Center and the Defense Department maintains the Joint Improvised Explosive Device Defeat Organization.

   a. What new capability does OBP provide the federal government?

   The Office of Bombing Prevention (OBP) currently exists within the Office of Infrastructure Protection; it is not a new office. OBP brings a strategic and overarching framework from which the United States Government can begin to address the IED threat. By working with interagency partners across the Federal government OBP is already addressing the IED threat in a holistic fashion.

   OBP is providing the strategic leadership essential for an effective national effort with national priorities. OBP will play a lead coordination role that will allow the Federal government to more effectively utilize our resources. Additionally, OBP leads the Counter IED IPT and response sub-IPT for DHS S&T in partnership with the U.S. Secret Service.

   Finally, OBP's role within the Office of Infrastructure Protection is essential to ensure the nation's people and infrastructure are protected by a coordinated national effort to reduce risk against the terrorist's primary weapon of choice.

   b. How does DHS intend to work with other agencies, especially Justice and Defense, to ensure there is no duplication of effort?

   OBP is already working with the interagency community to ensure there is no duplication of effort. I closely track OBP's progress and am focused on making strides to close gaps and ensure proper coordination. The OBP Advisory Group which is comprised of the interagency including members from DOJ and DoD as well as the private sector, is key to the coordination effort. This advisory group was used to create TRIPwire, write the Congressional Report as well as the HSPD-19 Report to the POTUS.

2. In response to Committee questions you state that you plan to convert contract staff to Federal staff "where appropriate to make the most efficient use of resources." You also indicate that the ratio of full time employees to contractors is almost 1 to 1 in the Office of Infrastructure Protection. The Chief Human Capital Officer at the Office of National Intelligence reports that his per capita annual cost for a contractor is $250,000 while the cost of a federal employee is $132,000. Are your per capita costs similar? Please provide that number for the record.

The average ratio of government FTE to contractors for NPPD is 1 FTE to 1.7 contractors. This was derived using a snapshot of FTEs as of September 2007. Additionally, if we assume that all authorized vacancies are filled (a top priority for NPPD) against the same contractor totals the ratio drops to 1 FTE to 1.25 contractors. NPPD's per capita FTE and contractor costs are in line with the example we were provided for the Office of National Intelligence ($132K per FTEs and $250K per contractor). The NPPD per capita costs for an FTE is approximately $133K and a contractor per capita cost is $243K.

3. In response to the Committee's pre-hearing questions, you state that the National Protection and Programs Directorate will soon be launching employee advisory councils. Please provide additional detail regarding these councils, including their membership, leadership and terms of reference.

I value the utilization of Employee Advisory Councils based on my previous experience. I have asked my Chief of Information Management and Business Culture to launch an NPPD Employee Advisory Council (EAC). Establishment of the EAC is genuine recognition of the value of an engaged workforce--a workforce that understands the mission of the Directorate, the distinct role each individual employee plays, and the contributions the various teams play in fulfilling the mission. Membership of the Council represents each of the NPPD components (IP, CS&C, US-VISIT, RMA, IGP) and core business support functions. The EAC serves in an advisory capacity to me and senior leadership. They serve as the conduit through which employees--at any and all levels--can express concerns, submit ideas for workplace or work process improvement, or question standard operating procedures. The EAC will identify employee workplace issues and work with me and Directorate leadership to mitigate or resolve problems. Ideally, the EAC is an effective mechanism for both improving employee communications and resolving employee workplace issues. The initial EAC membership has been determined and a kickoff meeting has been conducted. We are looking forward to the continued engagement with our workforce on the issues that are most important to them.

4. Airline collection and transmission of traveler fingerprints for US-VISIT raises serious privacy concerns. What privacy and security protections is the Department building into the program?

DHS is committed to the privacy of passenger data, as we are to protecting national security, and will ensure that the standards which the carriers will be required to meet will support this commitment. DHS will require strict compliance with specified methods of both collection and transmission of the biometric data which will help ensure that no privacy breaches occur. The transportation carriers will use a standards/technical guide developed by DHS for the APIS and Secure Flight data transmission requirements. The US-VISIT technical guidelines for submission of biometric data will be added to the guide and will clarify the guidelines for quality and security of the data that is collected,

transmitted and subsequently purged. DHS will institute audits of the transportation data systems to ensure compliance with the requirements.

5. In response to the Committee's pre-hearing questions, you state that the air exit system will be operation by the end of 2008. US-VISIT has experienced a series of delays and difficulties implementing an air exit system. Is the end of 2008 really a feasible time frame?

While the end of 2008 is an aggressive goal, it is a feasible timeframe for DHS to publish the regulation, ensure the technical guidelines are added to the standards document and provided to the transportation carriers, and complete DHS technical infrastructure development to receive and match the data and be ready to test with the carriers. I am meeting with the Director of US-VISIT and his staff weekly to ensure that we are aggressively working towards our milestones. I am also engaging DHS leadership as needed to leverage the Department's resources to assist us in meeting this timeframe and actively coordinate with the transportation companies. Since we are relying on the airlines to actually implement the exit program this will require their active participation and adherence to the regulations we publish.

Senator Susan M. Collins
Additional Questions for the Record
Nomination Hearing of Robert D. Jamison
November 9, 2007

1. The Post-Katrina Emergency Management Reform Act established the Office of Emergency Communications to coordinate efforts to attain interoperable communications at all levels of government. As we saw in the Hurricane Katrina disaster, a lot of work still needs to be done in this area, especially in assisting local first responders. What are you doing to strengthen this office and ensure that DHS does all it can to assist state and local governments in achieving interoperability?

   The Office of Emergency Communications (OEC) has an important role to play in coordinating interoperable communications at all levels of government. I have recently hired a Deputy Director of the OEC, Michael Roskind, who has 15 years of experience in the state, local and private sector working on law enforcement and communications issues. Mike has been on board for approximately 8 weeks now. And we will soon have a Director of OEC on board. The new Director will bring a wealth of experience as the leader of Virginia's interoperable communications efforts. These two key hires demonstrate we are working to build a strong team in OEC to carry out this important mission.

   The OEC is actively involved in the Fiscal Year 2008 Homeland Security Grant Program which provides needed financial resources to State and local governments to build or expand on their interoperable communications capabilities as well as other Homeland Security priorities.

2. In your pre-hearing questionnaire, you listed cyber security as one of your top three priorities if confirmed for this position. Cyber-security is just one of 17 different sectors of the economy that DHS is working with to protect our nation's critical infrastructure. Do you believe that cybersecuirty has not received sufficient attention given its importance to all sectors of our economy?

   The Department of Homeland Security through the CyberSecurity and Communications division of the National Protection and Programs Directorate has prioritized cybersecurity. We have a dedicated staff within the National Cyber Security Division , in particular within US-CERT, which is coordinating with the interagency community to ensure that cybersecurity is a top priority of every Federal government agency as well as state and local governments and the critical infrastructure owners and operators. As you note, given cybersecurity's importance to all sectors of our economy we will continue to invest in people and resources to strengthen our cybersecurity program. Our nation's dependence on the internet grows daily and the resolve to improve cyber security must continue to have a commensurate focus from the federal government.

3. Of the 17 sectors with which DHS works to protect critical infrastructure, cyber is probably the most diverse and unregulated. As an industry that has grown up only in the

last 20 to 30 years, it has led technological revolutions and continues to be a source of innovation for our economy. However, this constant change and hundreds of new actors appearing each year means that the government has very little visibility into the problems that exist in this sector. Few companies, whether as providers or customers, are willing to provide concrete data on the risks and vulnerabilities in their IT networks, precisely because those networks are so vital to business. How can we begin to build a solid set of data that allows us to identify the greatest vulnerabilities?

Under the National Infrastructure Protection Plan Sector Partnership Framework, we are working closely with the private sector, as well as with federal and state government stakeholders, to assess risk in the IT Sector. Since the development of the IT Sector Specific Plan and its release in May 2007, the IT Sector has been working collaboratively to decompose the sector's critical functions, and develop the consequence framework and threat taxonomy needed to initiate the top-down risk assessment appropriate for this unique sector. We are pleased that this initial phase has recently been completed, and we are about to begin the actual risk assessment of the IT sector, identifying vulnerabilities and assessing those vulnerabilities in the context of threat and consequence. Because our risk assessment methodology was created jointly with the IT Sector Coordinating Council, we have buy-in from our private sector stakeholders to conduct the actual risk assessment as a joint government-industry activity. We have structured our process to address concerns about exposure of proprietary data, and will utilize the protections of the Critical Infrastructure Partnership Advisory Council and Protected Critical Infrastructure Information as appropriate and necessary.

4. The recently reported Aurora scenario, a reference to the potential electrical generator vulnerability where a terrorist could use cyber networks to remotely attack and severely damage generators, poses a clear threat to our nation's infrastructure. I am encouraged by the Department's efforts to identify this vulnerability, develop counter-measures, and work with the private sector on this threat. I understand the Department was able to quickly reach out to each nuclear site and confirm the sector was aware of the threat and started implement corrective measures. I am, however, extremely concerned that the Department had difficulty confirming that the energy sector had been fully addressed this problem. If confirmed, how will you ensure that this threat is fully addressed by all critical infrastructure sectors? How will you ensure that future vulnerability information is better disseminated?

We must continue to get better at measuring the implementation of security measures in the field. This is a cross-cutting issue for NPPD that goes beyond cybersecurity measures. We will continue to closely monitor this threat and the sectors actions.

We are working with our partners in the Energy Sector on an ongoing basis to ensure mitigation of the Aurora vulnerability and to enhance control systems security in this critical sector in general. Because of the sensitivity of this issue, our outreach began with those sectors presenting the greatest risk, and that would be most directly affected by the vulnerability. While the Nuclear and Electric sectors were addressed first, DHS has continued its outreach to the second tier of potentially affected sectors, and worked

with the Chemical, Dams, Water, and Oil and Gas sectors to release mitigation plans for their industry owners and operators. We are continuing to work with other sectors to assess risk from this vulnerability to their operations and to develop and promulgate appropriate mitigation actions. In addition to our in-depth engagement with the individual sectors on this issue, DHS provided high level briefings and status updates to the leadership of all 17 CI/KR sectors through the Partnership for Critical Infrastructure Security and National Infrastructure Protection Plan Federal Senior Leadership Council. In addition, we are continuing to examine lessons learned from this issue to ensure that identified refinements are incorporated into the DHS information sharing process.

While we believe the sector partnership framework worked successfully in this instance to disseminate vulnerability and mitigation information that could be acted upon in a timely fashion, we are currently doing a lessons learned follow up with the nuclear and electricity sectors to identify measures that would enhance any future dissemination in similar circumstances.

5. The Chemical Facility Anti-Terrorism Standard (CFATS) program recently issued both a final rule and chemicals of interest (COI) list. The Department has taken an unprecedented approach to regulating an industry based on risk and proposes a "phased" implementation. Phase I would address the highest risk facilities. It is encouraging that the Department intends to move quickly and aggressively to implement this initial phase. However, the Department's guidance on implementing Phase II and Phase III is not clearly articulated. It is important the Department to implements a comprehensive regulatory program. What is the Department's plan for the implementation of Phase II and Phase III?

The chemical security program is being implemented in 2 Phases (not 3) both of which are already underway. The two phases correspond to the triggering requirements for completing a computer-based consequence assessment, known as a "top screen." Pursuant to the regulation, DHS can contact facilities directly and request that they complete the top screen or DHS can require facilities to complete the top screen based on their possession of certain chemicals at certain quantities as identified in the "DHS Chemicals of Interest" list.

Phase 1 was launched with the interim final rule, which DHS published in the Federal Register on April 9. This interim final rule became effective on June 8. in early June, DHS began notifying certain facilities directly that they had been determined to be potentially high risk, and so were required to complete a top screen. DHS selected these facilities by using existing data that led us to believe the facilities would be consequential enough to be regulated under the chemical security program. We will not have a complete understanding of the highest risk facilities until we complete an evaluation of the top screen process for the entire chemical sector.

Phase 2 is the execution of the Interim Final Rule as it relates to the "DHS Chemicals of Interest list, which is contained in Appendix A to the chemical security rule. With the

publication of a final list of chemicals of interest, facilities will have 60 calendar days to complete and submit a top screen to DHS. DHS released the final "Chemicals of Interest" list in early November and expects that it will be published in the Federal Register in mid-November.

Following completion of the top screen process, for both Phase I and Phase II of the CFATS program, DHS will make preliminary tiering determinations for "high risk" facilities. Facilities deemed to be high risk will be required to conduct vulnerability assessments. Following review of vulnerability assessments, DHS will make final tiering determinations for high risk facilities. At this time, high risk facilities will be required to create site security plans that must be approved by the Department, and implemented.

Testimony
W. Ross Ashley, III, Nominee
Assistant Administrator, Office of Grant Programs, Federal Emergency Management Agency,
Department of Homeland Security
United States Senate
Committee on Homeland Security and Governmental Affairs

November 9, 2007, 9:00 a.m., 342 Dirksen Senate Office Building

Good morning Mr. Chairman, Senator Collins, and Members of the Committee. My name is Ross Ashley. I'd like to thank Senator Warner for his statement of support.

I am appearing before you today as the nominee for Assistant Administrator for Grant Programs at the Federal Emergency Management Agency within the Department of Homeland Security. It is a great honor to be nominated by the President for this position and to have the opportunity to answer your questions as you consider my nomination. I cannot express enough how honored I am to be nominated for a position that will continue to further the preparedness, response and recovery capabilities of our State, local and tribal partners and the Nation as a whole.

I'd like to begin today by first thanking my wife Lauren for her patience and encouragement over the past ten years as our family has grown. As each of you know public service requires dedication and commitment from the whole family. Also with us today are our oldest daughter and two sons, Catherine, Cailan and Patrick who inspire me with the eagerness in which they approach the start of every day. Our two year old daughter Caroline thought best to hold down the fort while the rest of the family came for the hearing today. My mother is here from Alabama and I'd like to thank her for making the trip to be with us.

I have had the privilege of growing up in a family full of public servants. My father retired from serving both in the United States Air Force and the National Guard, and my mother worked in rural Mississippi as a social worker. My brother, Major John Ashley is here today from serving on active duty in the National Guard. John is the true picture of the citizen soldier having piloted F-16s on multiple combat deployments to Iraq and now preparing himself and others for deployment again in a new theater-based reconnaissance aircraft. John, his wife Tracy, and their four children's dedication to their country is an inspiration to all of us who know them.

If confirmed as Assistant Administrator for Grant Programs my responsibility will be to ensure that Federal investments into State, local and tribal preparedness, response and recovery capabilities provide the greatest return on investment for the American public. I will bring to this position many years of experience in military service, financial management and executive leadership.

I spent twenty years in the National Guard and Reserves serving both as an enlisted member and as a commissioned officer. Early in my National Guard career I volunteered on a number of occasions to fill sand bags and to pre-position supplies and equipment in order to prepare for hurricanes and floods threatening the Commonwealth of Virginia. Immediately following 9/11 as a reserve officer I volunteered to augment active duty personnel at the Pentagon manning a 24 hour intelligence watch center. From the time I was eighteen years old, the educational and professional opportunities afforded me in the National Guard have been the foundation for every endeavor in my life and, if confirmed, I will bring this foundation with me to this new challenge.

One of the most important aspects of this position is to ensure that Federal investments and partnerships with State, local and tribal first responders provide support to meet the National Preparedness Guidelines and the Target Capabilities List. This process requires financial experience in grant programs, fiscal responsibility and accountability.

Since 1997, I have had the opportunity to work as a commercial partner with State, local and tribal first responders specifically in the areas of information sharing, incident management and communications interoperability. As founder and President of The Templar Corporation I worked with individual States and localities on regional information sharing grants and supported all aspects of the grants process from interpretation of guidance, preparation of submission packages, and financial and programmatic compliance. If confirmed, I believe I will bring the necessary perspective of our State, local and tribal partners to the execution of all grant programs.

Prior to 9/11, I supported initial efforts to provide regional interoperable capabilities to our Nation's first responders. Shortly after the killing of Gianni Versace in 1997 it was discovered that his killer Andrew Cunanan pawned property under his real name while there was a nation-wide hunt underway for his apprehension. As a result of this and other multi-jurisdictional events I worked with the Department of Justice and other partners to develop a real-time distributed information sharing system for Broward, Brevard and Monroe Counties in South Florida. Since these early efforts I have had the opportunity to support similar interoperability efforts for both voice and data communications in a number of states and multi-jurisdictional regions to include the National Capital Region.

My financial management experience includes efforts with my business partner to mortgage our houses and start a successful small business, participating in complex multimillion dollar corporate sales both in the commercial and nonprofit sectors and leading a high performance financial management team in a turn around of a challenged nonprofit. As the CEO of an 1100 person nonprofit I was responsible for multiple cost centers and funding agencies at both the State and Federal level that cut across all aspects of the lives with people with developmental disabilities. When I took over as CEO of the National Children's Center the previous fiscal year audit included thirty-two findings of significant deficiency. Working with and leading a great team we were able to, in one short year, reduce the number of audit findings to two, neither of which was in the area of financial management.

It is also critical at this point to ensure that the resulting organizational changes in grant programs have a minimum affect on our stakeholders. Over the years working with states and localities, one of the common themes in grant programs is the need for consistency year over year. If confirmed, I will ensure that the transition to a one-stop-shop for grants continues to fully support all of our stakeholders. In addition, if confirmed, I am committed to an effective transition to the next administration and will ensure that my successor has all the tools necessary to continue the tremendous work already accomplished by this Congress and the Administration.

Our Nation's grant programs are critical to ensure adequate all-hazard planning and operational capabilities for emergency managers, firefighters, law enforcement, medical response and everyday citizens. If confirmed, I look forward to working with Administrator Paulison, the FEMA leadership team, across the Department of Homeland

Security and with all our partners continuing the efforts to develop a new FEMA and a culture of preparedness across our society.

In closing, the Congress continues to support the efforts of our Nation's first responders and has provided the necessary guidelines in the Post Katrina Emergency Reform Act of 2006 and the Implementing Recommendations of the 9/11 Commission Act. If confirmed, I welcome the opportunity to continue these efforts to support our Nation's first responders and respectfully ask this committee to confirm my nomination to serve as Assistant Administrator for Grant Programs at the Federal Emergency Management Agency within the Department of Homeland Security. I want to thank you Mr. Chairman for the opportunity to appear before you, and I would be happy to answer any questions you may have.

BIOGRAPHICAL AND FINANCIAL INFORMATION REQUESTED OF NOMINEES

A. BIOGRAPHICAL INFORMATION

1. **Name:** (Include any former names used.)

   Wiley Ross Ashley, III; W. Ross Ashley, III

2. **Position to which nominated:**

   Assistant Administrator Grant Programs

3. **Date of nomination:**

   26 June 2007

4. **Address:** (List current place of residence and office addresses.)

   REDACTED

5. **Date and place of birth:**

   25 September 1965
   Montgomery, Alabama

6. **Marital status:** (Include maiden name of wife or husband's name.)

   Married
   Wife: Lauren Catherine Ashley – Maiden Name: Lauren Catherine Dobuski

7. **Names and ages of children:**

8. **Education:** List secondary and higher education institutions, dates attended, degree received and date degree granted.

   Tabb High School – 1981 -1984, Diploma
   George Mason University – 1984-1988, BA December 1988
   Joint Military Intelligence College – 1993-1994, MS August 1994

9. **Employment record:** List all jobs held since college, and any relevant or significant jobs held prior to that time, including the title or description of job, name of employer, location of work, and dates of employment. (Please use separate attachment, if necessary.)

6/2007 – Present SRC, Inc; Senior Advisor to NIJ; Arlington, VA
1/2006 – 4/2007 National Children's Center; Chief Executive Officer; Washington, DC
2/2004 – 1/2006 ChoicePoint; Vice President; McLean, VA
2/2000 – 2/2004 Templar Corporation; Founder & President; Alexandria, VA
11/1995 – 1/2000 ISX Corporation; Director LE Technologies; Arlington, VA
1/1995 – 11/1995 Space Applications Corporation; Senior Tech Staff; Vienna, VA
2/1994 – 1/1995 Pacific Sierra Corporation; Program Analyst; Arlington, VA
1/1990 – 2/1994 Synergy, Inc.; Analyst/Manager; Washington, DC
6/1997 – 3/2004 Air Force Reserves; Intelligence Officer; Pentagon
3/1984 – 6/1997 Virginia Air National Guard; Intelligence Officer; Richmond, VA

10. **Government experience:** List any advisory, consultative, honorary or other part-time service or positions with federal, State, or local governments, other than those listed above.

None.

11. **Business relationships:** List all positions currently or formerly held as an officer, director, trustee, partner, proprietor, agent, representative, or consultant of any corporation, company, firm, partnership, or other business enterprise, educational or other institution.

Current positions:
Limited Partner, Braddock Hedge Fund
Previous positions:
The Templar Corporation, Officer and Director
National Children's Center, Vice President of the Board of Directors
National Children's Center, Chief Executive Officer

12. **Memberships:** List all memberships, affiliations, or and offices currently or formerly held in professional, business, fraternal, scholarly, civic, public, charitable or other organizations.

Army Navy Country Club – Current
International Association of Chiefs of Police – Current
Republican National Committee - Current
National Children's Center Board of Directors – No longer affiliated
Tau Kappa Epsilon Fraternity – No longer affiliated

13. **Political affiliations and activities:**

(a) List all offices with a political party which you have held or any public office for which you have been a candidate.

None.

(b) List all memberships and offices held in and services rendered to any political party or election committee during the last 10 years.

None.

(c) Itemize all political contributions to any individual, campaign organization, political party, political action committee, or similar entity of $50 or more during the past 5 years.

2004 President Bush - $2000
2006 Friends of George Allen - $1250
2006 Allen Victory Committee - $5000
2006 Asa Hutchenson (Arkansas Gov Race) - $250
2006 Mark Warner (PAC) - $1000
2007 RNC - $1000
2007 Mayor Adrian Fenty (DC Mayor Race) - $350
2007 Carol Green (Ward 4 DC Rade) - $500
2007 Vince Orange (DC Mayor Race) - $250

14. **Honors and awards:** List all scholarships, fellowships, honorary degrees, honorary society memberships, military medals and any other special recognitions for outstanding service or achievements.

Air Force Meritorious Service Medal
Air Force Commendation Medal
Air Force Achievement Medal
Air Force Longevity
National Defense Medal
Good Conduct Medal
Virginia National Guard Service Medal
Expert Marksman (2 devices)
Basic Military Academy Medal (2 devices)
Distinguished Graduate, Academy of Military Science
Distinguished Graduate, Target Intelligence Technical School

15. **Published writings:** Provide the Committee with two copies of any books, articles, reports, or other published materials which you have written.

Attached.

16. **Speeches:**

(a) Provide the Committee with two copies of any formal speeches you have delivered during the last 5 years which you have copies of and are on topics relevant to the position for which you have been nominated. Provide copies of any testimony to Congress, or to any other legislative or administrative body.

No formal speeches.

(b) Provide a list of all speeches and testimony you have delivered in the past 10 years, except for those the text of which you are providing to the Committee. Please provide a short description of the speech or testimony, its date of delivery, and the audience to whom you delivered it.

I have sat on a number of panels where no formal speech was given. In each case the topics were on three specific areas:
a) Information Sharing for Public Safety
b) Command and Control for First Responders
c) Role-based access control utilizing Public Key Infrastructures

17. **Selection:**

(a) Do you know why you were chosen for this nomination by the President?

I believe I was chosen for this nomination due to my diverse set of experiences and how these experiences match up with the needs of the Department of Homeland Security. I have had the opportunity to work with state and local governments across this Country on a variety of homeland security and public safety issues. I have worked with all levels and branches of state and local government from city councils and county boards of supervisors to mayors and governor's executive staff.

I also believe that my corporate experience in smart growth and change management were in a large part contributing factors to my nomination. As the new FEMA begins to mature as a result of the Post Katrina Reorganization Act having leadership in place experienced with change management and creating environments where people are encouraged to excel will be critical to the success of the agency.

(b) What do you believe in your background or employment experience affirmatively qualifies you for this particular appointment?

There are four key components in my background that make me uniquely qualified for the appointment:

Grants management experience
Financial management (small and large scale)
State and local government interaction

Leadership

For the past 10 years I have worked with a variety of grants systems and have supported a number of public safety and criminal justice clients as they have transitioned from ODP to DHS grant processes. As early as 1997 I worked with the Joint Program Steering Group (JPSG) to secure grants from OJP and NIJ to transition high payoff technologies to state and local first responders. These grants secured funding to move enabling technologies such as less than lethal, incident management and information sharing to the first responder community from the Defense Advanced Research Projects Agency (DARPA).

On a number of occasions I have worked and supported clients across the Country both in order to apply for and comply with grants from ODP, OJP, NIJ and DHS. Some specific examples of this are Hampton Roads CRIMES system, San Diego ARJIS and a number of projects with DOJ/NIJs NLECTC system. I also supported the California Anti-Terrorism Information Center (CATIC) by ensuring that a $4MM grant was appropriated by the State Legislature before expiration of the funding occurred.

I have a vast amount of financial management experience in areas such as mortgaging a house to start a small business, raising private equity funding, negotiating a multi-million dollar sale, supporting another multi-million dollar sale and running a multimillion dollar non-profit with numerous cost centers.

Obviously a lot of my large scale financial management experience is from the private sector however as I mentioned in the grants management experience section I helped agencies comply with grants to include the financial management reporting process. In addition I have worked with agencies to apply for grants and aided with the cost proposal sections of these applications.

One of the things that excites me the most about this appointment is the chance to work once again with state and local governments and the first responders that support these communities. Most recently, in 2004 and 2005 I ran relationship management for all state and local data and information sharing accounts for ChoicePoint. In this capacity I interacted with and traveled to nearly every major jurisdictional and multi-jurisdictional task force throughout the United States.

On many occasions I supported the first responder community by working with City Councils, County Boards and State Legislatures. Many of these instances were to ensure stakeholder acceptance of information sharing within the communities.

I have had the opportunity to perform in a variety of leadership positions throughout my career. Most recently, I had the opportunity to lead a financially challenged non-profit as the Chief Executive Officer. In this capacity I was responsible for over 1,100 employees working in diversified fields. As the Chief Executive Officer I was responsible for leading all aspects of the agency from education, residential services, transportation, facilities, medical staff, day treatment, early intervention as well as to ensure that 5 retail

thrift stores were able to offset cash flow requirements in the consolidated budget. Prior to my arrival there was not an effective budget process and no senior leadership team in place. Over the year and a couple of months I was there I ensured that a leadership team was in place and that the budget process included a bottom up analysis from the individual cost centers and would live beyond my tenure there.

All of the above experiences, coupled with 20 years of military experience, provide me with a diverse set of qualifications in order to provide the Department of Homeland Security the necessary leadership to administer grants programs within the Federal Emergency Management Agency.

B. EMPLOYMENT RELATIONSHIPS

1. Will you sever all connections with your present employers, business firms, business associations or business organizations if you are confirmed by the Senate?

   Yes.

2. Do you have any plans, commitments or agreements to pursue outside employment, with or without compensation, during your service with the government? If so, explain.

   No.

3. Do you have any plans, commitments or agreements after completing government service to resume employment, affiliation or practice with your previous employer, business firm, association or organization, or to start employment with any other entity?

   No.

4. Has anybody made a commitment to employ your services in any capacity after you leave government service?

   No.

5. If confirmed, do you expect to serve out your full term or until the next Presidential election, whichever is applicable?

   Yes.

6. Have you ever been asked by an employer to leave a job or otherwise left a job on a non-voluntary basis? If so, please explain.

   No.

C. POTENTIAL CONFLICTS OF INTEREST

1. Describe any business relationship, dealing or financial transaction which you have had during the last 10 years, whether for yourself, on behalf of a client, or acting as an agent, that could in any way constitute or result in a possible conflict of interest in the position to which you have been nominated.

   ChoicePoint bought my company (The Templar Corporation) in 2004. I do not own any ChoicePoint stock and do not have any other financial relationships with the Company or any of their employees, officers or directors. I do not view this as a conflict of interest but would understand how it could possibly be viewed out of context.

2. Describe any activity during the past 10 years in which you have engaged for the purpose of directly or indirectly influencing the passage, defeat or modification of any legislation or affecting the administration or execution of law or public policy, other than while in a federal government capacity.

   None.

3. Do you agree to have written opinions provided to the Committee by the designated agency ethics officer of the agency to which you are nominated and by the Office of Government Ethics concerning potential conflicts of interest or any legal impediments to your serving in this position?

   Yes.

D. LEGAL MATTERS

1. Have you ever been disciplined or cited for a breach of ethics for unprofessional conduct by, or been the subject of a complaint to any court, administrative agency, professional association, disciplinary committee, or other professional group? If so, provide details.

   No.

2. Have you ever been investigated, arrested, charged or convicted (including pleas of guilty or nolo contendere) by any federal, State, or other law enforcement authority for violation of any federal, State, county or municipal law, other than a minor traffic offense? If so, provide details.

   No.

3. Have you or any business of which you are or were an officer, director or owner ever been involved as a party in interest in any administrative agency proceeding or civil litigation? If so, provide details.

Yes, civil suit on one occasion.

4. For responses to question 3, please identify and provide details for any proceedings or civil litigation that involve actions taken or omitted by you, or alleged to have been taken or omitted by you, while serving in your official capacity.

   Litigation was not due to any actions taken or omitted by myself. The situation was the result of an oversight by ChoicePoint to cancel a lease on a phone system once they acquired Templar. Due to the lease not being canceled it automatically renewed in a location ChoicePoint had closed. Once ChoicePoint was made aware of the suit they resolved the matter immediately. I was named on the suit as a guarantor of the original lease.

5. Please advise the Committee of any additional information, favorable or unfavorable, which you feel should be considered in connection with your nomination.

   My military experience as an intelligence officer in the National Guard and Reserve should also be considered favorably. As an intelligence officer and a contractor for the Department of Defense I was afforded opportunities to work with threat-based analytical systems as well as cost to capability modeling systems. Each of these systems focused on resource allocation in a constrained fiscal environment.

E. FINANCIAL DATA

All information requested under this heading must be provided for yourself, your spouse, and your dependents. (This information will not be published in the record of the hearing on your nomination, but it will be retained in the Committee's files and will be available for public inspection).

AFFIDAVIT

W. Ross Ashley III being duly sworn, hereby states that he/she has read and signed the foregoing Statement on Biographical and Financial Information and that the information provided therein is, to the best of his/her knowledge, current, accurate, and complete.

Subscribed and sworn before me this 10th day of July, 20 07

Notary Public

Michelle D. Parrish
Notary Public, District of Columbia
My Commission Expires 11-14-2007

U.S. Senate Committee on Homeland Security and Governmental Affairs
Pre-hearing Questionnaire
For the Nomination of Wiley Ross Ashley, III to be
Assistant Administrator for Grant Programs, Federal Emergency Management Agency,
Department of Homeland Security

I. Nomination Process and Conflicts of Interest

1. Why do you believe the President nominated you to serve as Assistant Administrator for Grant Programs?

ANSWER:

I believe I was chosen for this nomination due to my unique professional background and diverse set of experiences. I have had the opportunity to work with State and local governments across this country on a variety of homeland security and public safety issues. I have worked with all levels and branches of State and local government from city councils and county boards of supervisors to mayors and governors' executive staff.

I also believe that my corporate experience in smart growth and change management were significant contributing factors to my nomination. As the New FEMA begins to mature as a result of the Post Katrina Emergency Management Reform Act of 2006 (PKEMRA), having leadership with strong change management skills and the ability to create environments where people are encouraged to excel will be critical to the success of the agency.

2. Were any conditions, express or implied, attached to your nomination? If so, please explain.

ANSWER:

None

3. What specific background and experience affirmatively qualifies you to be Assistant Administrator for Grant Programs?

ANSWER:

For the past ten years I have worked with a variety of grants programs and have supported a number of public safety and criminal justice clients as they have transitioned from the Office of Domestic Preparedness (ODP) to the Department of Homeland Security (DHS). As early as 1997, I worked with the Joint Program Steering Group (JPSG) to secure grants from the Office of Justice Programs (OJP) and the National Institute of Justice (NIJ) to transition high payoff technologies to

State and local first responders. These grants secured funding to move enabling technologies such as less than lethal, incident management and information sharing to the first responder community from the Defense Advanced Research Projects Agency (DARPA).

On a number of occasions I have worked with and supported clients from across the country to help them to apply for and comply with grants from ODP, OJP, NIJ and DHS. Specific examples include Hampton Roads' Comprehensive Regional Information Management and Exchange System (CRIMES), San Diego's Automated Regional Justice Information System (ARJIS) and a number of projects with DOJ/NIJ's National Law Enforcement and Corrections Technology Center (NLECTC). I also supported the California Anti-Terrorism Information Center (CATIC) by ensuring that a $4 million grant was appropriated by the State legislature before expiration of the funding occurred.

I have a vast amount of financial management experience in areas such as raising private equity funding, mortgaging a house to start a small business, negotiating and supporting multi-million dollar sales and running a multimillion dollar non-profit with numerous cost centers.

Though a significant amount of my large-scale financial management experience is in the private and nonprofit sectors, much of my past experience supported agencies in order to comply with grants to include the financial management reporting process. In addition I have worked with agencies to apply for grants and aided with the cost proposal sections of these applications.

One of the things that excites me the most about this appointment is the chance to work once again with State and local governments and the first responders that support these communities. Most recently, in 2004 and 2005 I ran relationship management for all State and local data and information sharing accounts for Choicepoint. In this capacity I interacted with and traveled to nearly every major jurisdictional and multi-jurisdictional task force throughout the United States. On many occasions I supported the first responder community by working with City Councils, County Boards and State legislatures. Many of these instances were to ensure stakeholder acceptance of information sharing within the communities.

I have had the opportunity to perform in a variety of leadership positions throughout my career. Most recently, I had the opportunity to lead a financially challenged non-profit as the Chief Executive Officer. In this capacity I was responsible for over 1,100 employees working in diversified fields. As the Chief Executive Officer I was responsible for leading all aspects of the agency from education, residential services, transportation, facilities, medical staff, day treatment, early intervention as well as ensuring that five retail thrift stores were able to offset cash flow requirements in the consolidated budget. Prior to my arrival there was no effective budget process and no senior leadership team in place. Over the course of my time there, I ensured that a

leadership team was in place and that the budget process included a bottom up analysis from the individual cost centers and would live beyond my tenure there.

All of the above experiences, coupled with twenty years of military experience, provide me with a diverse set of qualifications in order to provide DHS the necessary leadership to administer grants programs within FEMA.

4. Have you made any commitments with respect to the policies and principles you will attempt to implement as Assistant Administrator for Grant Programs? If so, what are they, and to whom were the commitments made?

ANSWER:

None

5. If confirmed, are there any issues from which you may have to recuse or disqualify yourself because of a conflict of interest or the appearance of a conflict of interest? If so, please explain what procedures and/or criteria you will use to carry out such a recusal or disqualification.

ANSWER:

As expressed in my ethics statement, I have ended my employment with the National Children's Center less than one year ago and pursuant to 5 C.F.R. ξ 2635.502, and for one year will not participate in any particular matter involving specific parties in which National Children's Center is a party or represents a party, unless I am authorized to participate. To my knowledge the National Children's Center has never applied for grants under any DHS program.

Effective November 1, 2007, I will resign my current position as Senior Analyst for Scientific Research Corporation. Furthermore, pursuant to 5 C.F.R. ξ 2635.502, for one year after this resignation, I will not participate in any particular matter involving specific parties in which Scientific Research Corporation is a party or represents a party, unless I am authorized to participate.

ChoicePoint, Inc. bought my company (The Templar Corporation) in February of 2004. I do not own any ChoicePoint stock and do not have any other financial relationships with the Company or any of their employees, officers or directors. I do not view this as a conflict of interest but would understand however it might be considered an appearance of a conflict of interest.

As disclosed in my ethics agreement, I will divest of all holdings in the Braddock Hedge Fund. I do not view this fund as a conflict of interest however due to the proprietary nature of the fund and the holding of undisclosed positions it will be necessary for me to divest.

These abovementioned potential conflicts of interest have been made in conjunction with the Department's Designated Agency Ethics Advisor (DAEO) and the Director, U.S. Office of Government Ethics, and are contained in my ethics agreement. The agreement has been provided to the Committee along with my Public Financial Disclosure Report, SF 278. Should I be confirmed, I will work closely with the DAEO to ensure I avoid being involved in these matters or any other that present a conflict or an appearance of a conflict of interests.

6. Have you ever been asked by an employer to leave a job or otherwise left a job on a non-voluntary basis? If so, please explain.

ANSWER:

No.

II. Background of the Nominee

7. Have you ever previously administered, or participated in the administration of, any grant program? If so, please describe in detail your experience, including the nature of the grant program or programs and your role and responsibilities with respect thereto.

ANSWER:

Although I have never administered a grant program as an employee of the Federal or State government I have had the opportunity to work with numerous grant recipients from across the country. I have also participated in multiple types of grant programs and have worked as a team member both in formal and informal support roles. In many cases I have been asked to aide in the completion of grant applications, components of statewide homeland security plans and to provide competitive advice in interpreting grant guidance.

Given my experiences in the commercial sector working with first responders and in the National Guard I feel that I will bring the perspective of State and local grant recipients to the position. I believe that these perspectives are critical to the process of administering national grant programs. Understanding that jurisdictions and regions are unique in the types of challenges they may face and that the types of laws and business practices vary is ever important to meeting unique regional needs while still ensuring an effective return on investment of Federal tax dollars.

Additionally I believe that my financial qualifications in small and large scale financial management coupled with my State and local perspective will be of great benefit to DHS and provides the best mix of experiences to provide our non-Federal partners with world class grant administration and support.

8. Please describe in detail any other experience you have with homeland security grants, first responder grants, or other grants. For each item listed, please indicate the following:

   a. the grant or grant program involved;

   b. the entity providing the grants and/or administering the grant program;

   c. if applicable, the recipient of, or applicant for, the grant and the size of the grant received or applied for;

   d. the capacity in which you were involved with the grant or grant program, including the company or other entity with which you were employed, the position you held with that company or other entity at the time, and the company's or other entity's relationship to the grant or grant program; and

   e. your role and responsibilities with respect to the grant or grant program.

ANSWER:

For each of the following grant programs, with the exception of grants awarded to the Integrated Justice Information System (IJIS) Institute, The Templar Corporation was the prime contractor selected for technical implementation. The only exception was the CAPWIN program where Templar performed under a sub contract to IBM Corporation. As the contractor, I directly supported State and local grantees throughout the grant life cycle.

Performance on the IJIS Institute grants was on a volunteer basis. Efforts were focused on providing technical assistance to State and local public safety agencies in the areas of information sharing and interoperable communications.

Program Name: South Florida Information Sharing System
Grant Provider: National Institute of Justice jointly with DARPA
Grant Recipient: Broward, Brevard, and Monroe Counties, Florida
Grant Size: $900,000
Personal Role: Director of Law Enforcement Technologies – ISX Corporation
Grant Responsibilities: Application process, financial reporting and grant execution

Program Name: San Diego ARJIS Global Query
Grant Provider: National Institute of Justice
Grant Recipient: San Diego ARJIS
Grant Size: Multiple awards over four year period - $1.4 million
Personal Role: Founder, Templar Corporation
Grant Responsibilities: Application process, financial reporting, progress reporting and grant execution

Program Name: Domestic Violence Communication System
Grant Provider: National Institute of Justice
Grant Recipient: San Diego ARJIS
Grant Size: $250,000
Personal Role: Founder, The Templar Corporation
Grant Responsibilities: Financial reporting and grant execution

Program Name: Hampton Roads CRIMES
Grant Provider: The Community Oriented Policing Services (COPS) Program
Grant Recipient: 7 Jurisdictions in Virginia to include Norfolk and Hampton
Grant Size: $1 million
Personal Role: Founder, The Templar Corporation
Grant Responsibilities: Application process, financial reporting, progress reporting and grant execution

Program Name: Oregon Criminal Justice Information Sharing System
Grant Provider: National Institute of Justice
Grant Recipient: Oregon State Police
Grant Size: $250,000
Personal Role: Founder, The Templar Corporation
Grant Responsibilities: Application process, financial reporting, progress reporting and grant execution

Program Name: Low Country Information Sharing System
Grant Provider: National Institute of Justice
Grant Recipient: National Law Enforcement and Corrections and Technology Center, Southeast
Grant Size: $2 million
Personal Role: Founder, The Templar Corporation
Grant Responsibilities: Grant execution

Program Name: Drivers License Image Retrieval System
Grant Provider: Department of Criminal Justice Services, Florida
Grant Recipient: Florida Department of Law Enforcement
Grant Size: $100,000
Personal Role: Founder, The Templar Corporation
Grant Responsibilities: Financial reporting and grant execution

Program Name: Single Point Inquiry Criminal Exchange System (SPICES)
Grant Provider: COPS
Grant Recipient: CA Department of Justice, CATIC
Grant Size: $2 million
Personal Role: Founder, The Templar Corporation
Grant Responsibilities: Application process, financial reporting, progress reporting and grant execution (most of the execution occurred after my involvement)

Program Name: Florida's Online Criminal User System (FOCUS)
Grant Provider: National Institute of Justice
Grant Recipient: Office of Statewide Intelligence, Florida
Grant Size: $200,000
Personal Role: Founder, The Templar Corporation
Grant Responsibilities: Application process, financial reporting, progress reporting and grant execution

Program Name: Hampton Roads' CRIMES
Grant Provider: Department of Criminal Justice Services, Virginia
Grant Recipient: York County and Williamsburg, Virginia
Grant Size: $50,000/year for three years
Personal Role: Founder, The Templar Corporation
Grant Responsibilities: Application process and grant execution

Program Name: Capitol Area Wireless Integrated Network (CAPWIN)
Grant Provider/Funding Provider: Funded by DOT, NIJ and other entities
Grant Recipient: CAPWIN Program Office, U. of Maryland
Grant Size: Unknown
Personal Role: Founder, The Templar Corporation
Grant Responsibilities: Grant execution

Program Name: Arkansas Criminal Justice Information Sharing System
Grant Provider: Byrne Memorial Grant
Grant Recipient: Arkansas Department of Criminal Justice
Grant Size: $480,000
Personal Role: Founder, The Templar Corporation
Grant Responsibilities: Grant execution

Program Name: Integrated Justice Information System (IJIS) Institute Technical Assistance
Grant Provider: Bureau of Justice Assistance
Grant Recipient: IJIS Institute
Grant Size: Multiple years at less than $100,000 – current funding unknown
Personal Role: Founding Member, IJIS Institute
Grant Responsibilities: Technical Assistance

All of the dollar figures above are estimated to the best of my recollection.

9. Please describe in detail any other relevant homeland security experience you have, including but not limited to any experience you have in preventing, preparing for, protecting against, responding to, recovering from or mitigating against natural disasters, acts of terrorism, or other man-made disasters.

ANSWER:

I have had a variety of relevant homeland security experiences throughout my career as a member of the National Guard and Reserve. Early in my career I volunteered on a few occasions to prepare for hurricanes threatening the Virginia and North Carolina coast. As an enlisted member in the National Guard I filled countless sand bags and worked to preposition supplies prior to storm arrival.

Immediately following 9/11 as a member of the Reserves I volunteered to provide intelligence assessments and to man a 24/7 intelligence watch at the Pentagon augmenting active duty staff. In this capacity, I provided a number of classified terrorist assessments to the Air Force Chief of Staff.

As the founder of the Templar Corporation I worked with a number of states to include California and Florida to form statewide and regional fusion efforts. These efforts have become the initial basis for what we now call fusion centers. On many occasions I was called upon to evaluate the tools, technologies and processes employed by these statewide and regional efforts in order to provide assessments to operational leadership on effectiveness.

As the Chief Executive Officer of the National Children's Center I was responsible for the safety and security of over 600 clients each day. These clients took part in educational, residential, supervised day and transportation programs offered by the center. Working with the Nonprofit Roundtable of Greater Washington I began the process of developing a disaster and continuity of operations plan for the center across all of our programs. I also worked with the Mental Retardation and Developmental Disabilities Administration (MRDDA) to ensure that it was aware of the fleet of specialized busses and vans we would have during any necessary evacuation. As part of this overall process we were able to ensure that our schools and residential programs had the necessary information and supplies to shelter in place or evacuate if required.

Immediately following Hurricane Katrina I worked on providing residential placement for displaced persons with developmental disabilities. I also supported the move back to Louisiana of persons wishing to return home.

III. Role and Responsibilities of the Assistant Administrator for Grant Programs

10. Why do you wish to serve as the Assistant Administrator for Grant Programs?

ANSWER:

I wish to serve as the Assistant Administrator for Grant Programs due to the utmost respect I have for people serving in the first responder community. For the past twelve years I have had the privilege to work with first responders as a vendor and as

a consultant. I believe that my experiences in positions in the military, corporate leadership, and financial management will enable me to contribute to a continuous improvement process in DHS grant programs.

I also believe that grant programs are part of a critical mission area to provide overall homeland security capabilities at the State and local level. I am confident that my experiences will ensure that this critical mission is part of an overall successful transition to the next Administration.

11. What do you see as the principal mission(s) of the Office of Grant Programs?

ANSWER:

In my observations, the Grant Programs Directorate (GPD) is a grants organization that personifies the New FEMA. GPD encompasses both the program and business aspects of grants management, and therefore has a very unique and ambitious mission, which, if confirmed I hope to achieve. GPD's critical mission is to assist State and local entities in employing core grant programs and risk management frameworks to achieve homeland security capability targets, while also providing a unified, solutions-oriented approach to Federal financial assistance management in support of FEMA's multi-faceted mission, priorities and customer base.

12. What do you see as the Office of Grant Programs' principal strengths and weaknesses in its ability to accomplish those mission(s)?

ANSWER:

Without a doubt, the greatest strength of GPD is the commitment and expertise of its leadership and personnel. It is apparent that its staff is dedicated to the success of FEMA's programs and grantees, the leadership's vision, and most of all, to supporting one another. I find it remarkable and a testament to the caliber of the staff that they were able to stand up a new Directorate without its organic political and executive leadership and with no additional resources—monetary or otherwise.

The reputation of the Directorate's outreach efforts speaks for itself. This is one set of staff in the government that really works to be proactive with its constituents. Based on my experience in hearing from the Directorate's customers, the relationships built with people in the field, whether that be State, local, or other FEMA colleagues is first rate. If I am honored with this position, I am confident in a staff that I have not even met yet, based on their customers' feedback, and not many leaders have the chance to say that.

With strengths come challenges and leading a newly formed Directorate still in a transition period has challenges. The fact that the GPD is still in its infancy presents its own set of challenges. While those that have been or are in acting capacities have done an outstanding job, I believe providing corporate leadership for this high-

performing staff is key to the Directorate's continued mission success. As I said before, GPD's transitional leadership made great strides with this organization and if confirmed, I will continue the pace they have set and accelerate the work they have started.

13. What is your understanding of the division of grants-related responsibilities between the Office of Grant Programs and the National Preparedness Directorate?

ANSWER:

The missions and functions of GPD and the National Preparedness Directorate (NPD) are inextricably intertwined, thus requiring concerted and ongoing coordination between the personnel that make up these organizations. Effectively, the grant programs that are part of the GPD portfolio are a key vehicle through which the national preparedness initiatives designed through NPD can be implemented at the State and local level. NPD activities cannot effectively be achieved without leveraging the grants managed through GPD; and GPD programs require the strategic input from NPD on national preparedness priorities to focus each grant program.

GPD is responsible for developing, implementing, and monitoring a broad portfolio of preparedness grant programs that cut across prevention, protection, response, and recovery capabilities. This includes (but is not limited to) such programs as the Homeland Security Grant Program, the Infrastructure Protection Program, and the Emergency Management Performance Grant program. GPD staff builds the guidance that governs these grant programs and tracks performance throughout the life-cycle of the grants from both a programmatic and financial standpoint.

If confirmed, I would expect to have the lead for building the grant processes and products and executing the programs to ensure they support the national preparedness requirements identified in the National Preparedness Guidelines (NPG), the Post Katrina Emergency Management Reform and 9/11 Acts, and meet the needs of our grant recipients. If confirmed, I look forward to working closely with the Administrator and Deputy Administrators to support our national homeland security and related strategies, and commit to working closely with our partners in the Transportation Security Agency (TSA) and the United States Coast Guard (USCG). I will closely coordinate with these key partners throughout program life cycles to ensure grant programs, grant management tools, financial controls, audits and program management fully support achieving the vision of the NPG.

NPD is responsible for building the national preparedness policy and doctrinal framework. This includes a range of activities including training, exercises, incident management systems, national assessments, capability-based technical assistance, and the overarching preparedness policy considerations that guide these initiatives. NPD staff is responsible for designing common approaches to achieving and measuring national preparedness.

I plan to work closely with all Directorates within FEMA and with external partners to align our respective roles and to ensure our stakeholders are served by programs that support FEMA's multi-faceted mission, priorities and customer base.

IV. Policy Questions

General

14. If confirmed, what would be your top priorities? What do you hope to have accomplished at the end of your tenure?

ANSWER:

If confirmed, I hope to continue the efforts of the Department to work with State and local communities to identify capability gaps, utilize grant programs to further State and local capacities to prevent, protect, respond to and recover from a terrorist or man-made event, and to target outcome based planning as a priority. As you know, grant programs are a very important part of the homeland security and preparedness mission as they can assist in building a capability and meet strategic objectives. Fiscal Year 2008 grant programs will mark the third year in a row where the focus of the programs has been on the implementation of the NPG, which is centered around providing a structure for State and local governments to identify areas of capability and to target limited resources towards the highest areas of need.

My top priorities will be to strengthen the relationships already built with State and local communities to identify better ways to develop grant program guidance and the implementation of that guidance through monitoring and technical assistance. I also hope to feed off the momentum of the past few Fiscal Years where the grant programs have had tremendous outreach to their Federal partners for feedback and input on the grant program guidance and structure.

I also want to maintain a strong sense of continuity of the grant programs from year to year. DHS has heard from many of its State and local partners over the years that the programs shift and change far too much from year to year. I would not only want to listen to that feedback, but demonstrate by deed that we will quickly act on it. I would rank that point as one of my top priorities as we move into the Fiscal Year 2008 grant cycle and beyond.

By the end of my tenure, I hope to have worked with State and local communities to assist them in their preparedness efforts and to continue the development of strong strategic and outcome based investments for homeland security grant funds. I hope to have been successful in helping guide the Administrator's vision of the New FEMA. I hope to have been successful in instilling and implementing a common vision for GPD which is to be a recognized leader valued for proactive Federal assistance management that prepares the American public and supports them in their times of

greatest need. And, finally and unequivocally, I hope to do what people come to FEMA to do… and that is to make a difference in people's lives.

15. The Department of Homeland Security (DHS) is reportedly revising its strategic plan, which was issued in 2004, and the Federal Emergency Management Agency's (FEMA) strategic plan only covers the years 2003-2008.

    a. If you were asked to contribute to revised versions of these documents, what would you propose as the principal strategic goals and objectives of the Office of Grant Programs?

ANSWER:

I understand that FEMA's revised strategic plan should reflect its broader preparedness mission, including an influx of homeland security grant, technical assistance, training, exercise, and planning preparedness initiatives that are designed to counter all hazards.

Specifically, the strategic goals and objectives of GPD should be to integrate FEMA's many disaster and non-disaster grant programs into an efficient and consistent means to provide financial assistance based on risks and need. GPD should be a major tool for FEMA to integrate its missions to enhance capabilities to prevent, protect and mitigate against, respond to, and recover from all hazards.

    b. What performance indicators and associated measures would you propose be used to assess these goals and objectives?

ANSWER:

If confirmed, I will ensure our performance is ultimately measured against the contribution our programs, services and activities make to achievement of the NPG, the national preparedness priorities, and the specific requirements outlined in PKEMRA and The Implementing the 9/11 Commission Recommendations Act of 2007.

16. In approximately 15 months, there will be a new presidential administration and, presumably, new leadership of the Department of Homeland Security. What actions do you intend to take to ensure that there is a smooth transition to your successor and that the grants process is operating, and will continue to operate, effectively through the transition?

ANSWER:

First and foremost, I will ensure that there is adequate permanent career executive and other senior leadership positions in place to continue to provide stability upon my departure. Secondly, I plan to finalize the business processes that my colleagues have

been working on in the seven months since the inception of GPD and ensure that all policies and procedures are adequately documented. Lastly, I would hope for the opportunity to have time with my successor in the office, meeting with my staff and working through important initiatives that are pending. I understand it is often the case that political appointees have little transition interaction, but grant programs are of such critical importance to our nation's security that I commit to ensuring the transition provides all the safeguards to avoid disruption to these security sensitive programs. In order to ensure a smooth transition for core grant programs, adequate time with at least my successor's key staff is imperative.

Most of all, it is imperative for the next Administration and FEMA's career workforce to have a clear understanding of the Agency's organization structure and functional operations to maintain a high level of customer service for its stakeholders and a continuation of critical homeland security programs. I also intend to make available a detailed project plan of ongoing change initiatives, such as the consolidation of grant management systems into a common framework to ensure that milestones are met and investments are not lost.

Efficacy of Grants

17. Homeland security grants are the principal means the Department has to ensure that State and local governments – and therefore we, as a Nation – are prepared for all hazards, whether natural or man-made. This year, FEMA will distribute over $3 billion to State and local governments, port and transportation system operators, and first responders. How will you ensure these grants are effectively building our national capabilities to respond to – and, in the case of terrorist attacks and other manmade incidents, prevent – disasters?

ANSWER:

Based on publicly accessible information about the FY2007 grant application cycle, and the recent release of the NPG, I believe significant progress has been made to ensure grant programs are targeted at achieving the NPG and national preparedness priorities. I am aware of the extensive work DHS has accomplished with counterparts across levels of government to adopt an all-hazards, capabilities-based planning approach for national preparedness. I believe that is the appropriate way to balance two portfolios of risk – terrorism and natural hazards. Using our grants to build agile, flexible, robust and interchangeable all-hazards capabilities compensates for the high degree of uncertainty regarding the adaptive (terrorism) challenges we face (including the strong potential for surprise), and covers the wide range of natural hazards we frequently experience.

If confirmed, my role will include ensuring grant program reporting such as the Initial Strategy Implementation Plan (ISIP) and Biannual Strategy Implementation Report clearly outline how recipients are using grant funding to meet national goals and objectives and their State and Urban Area Homeland Security Strategies. I would

expect to have the responsibility to ensure the grant application process includes specific requirements to align applications and investment justifications with the NPG and national priorities, and that peer reviews ensure submissions are reviewed for alignment with national priorities.

I believe the PKEMRA requirement in Section 649 to establish a comprehensive assessment system is critical to gauge capability levels, resource needs, and performance of training, exercises, and operations. I understand that FEMA and its partners across the homeland security / emergency management community have been working on several pilot efforts related to assessment tools and systems. If confirmed, I will support these efforts to ensure they provide the means to conduct accurate assessments and report results in a meaningful and understandable way to Congress, the President, and the American people.

18. Section 652 of the Post-Katrina Emergency Management Reform Act of 2006, (P.L. 109-295, Title VI) (Post-Katrina Act), requires that FEMA submit to Congress an annual federal preparedness report that includes an assessment of how federal grant assistance supports the national preparedness system. The Implementing Recommendations of the 9/11 Commission Act of 2007, (P.L. 110-53) amends this provision to also require an evaluation of the extent to which grants administered by the Department have contributed to the progress of State, local and tribal governments in achieving target capabilities and have led to the reduction of risk from natural disasters, acts of terrorism, or other man-made disasters. In addition, States are required to provide to the FEMA Administrator each year an assessment of their current capability levels and the resources needed to meet preparedness priorities.

    a. What metrics will or should be used to assess the effect of grants on national preparedness and risk reduction?

    ANSWER:

    The Target Capabilities provide performance measures that serve as a basis for assessment. As I understand it, FEMA is making significant strides in developing the tools that that will form the basis for assessments of State and national preparedness. The effort to develop Target Capabilities and performance measures complements and incorporates the use of existing metrics, such as those identified in National Fire Protection Association (NFPA) 1600, the Standard on Disaster/Emergency Management and Business Continuity Programs. Homeland Security Presidential Directive-8 identified the requirement to develop "readiness metrics and elements that support the National Preparedness Goal (now Guidelines), including standards for preparedness assessments and strategies." PKEMRA requires employment of capability targets and establishes a series of periodic reports on State and national preparedness.

In addition, PKEMRA directed FEMA to establish a National Preparedness System. This system will synchronize operational and strategic planning processes, leverage resources, and exercise capabilities. This System will also assess the effectiveness of grant allocation toward risk reduction. The NPD will take the lead on establishing a robust National Preparedness System and with it assess the effectiveness of grants as they contribute to the objective of the Preparedness Guidelines. If confirmed, I will ensure that the GPD works closely with the NPD to ensure that grants are effectively leveraged to reduce risk.

Clear, consistent and measurable metrics are critical to providing investment feedback into the capability planning system. If confirmed, I will ensure that investments for all-hazard preparedness functions are measurable against Target Capabilities and I will fully support the efforts of the NPD in developing the federal preparedness report.

b. What metrics will or should FEMA require that States use to assess their current capability levels?

ANSWER:

As I understand and have observed, each of the current target capabilities include a description of the major activities performed with the capability and the critical tasks and measures associated with the activity. They include both preparedness and performance activities, tasks, and measures. The Target Capabilities List (TCL) describes preparedness activities and tasks as those things that should be done prior to the demand for the capability, such as development of plans, procedures, protocols, and systems, or establishment of mutual aid agreements and authorities. Performance activities and tasks are described as the actions taken to prevent, protect against, respond to, or recover from an actual event or are demonstrated during an exercise. Performance measures are quantitative or qualitative levels against which achievement of a task or capability outcome can be assessed. They describe in the TCL how much, how well and/or how quickly an action should be performed and are typically expressed in ways that can be observed during an exercise or real event.

c. The federal preparedness report required under section 652 of the Post-Katrina Act was due October 4, 2007 but has not yet been received by Congress. When do you anticipate that that report will be submitted to Congress? If confirmed, will you commit to working to ensure that that report is submitted expeditiously?

ANSWER:

The Post-Katrina Act mandated that a Federal Preparedness Report be prepared annually to inform Congress on the Nation's level of preparedness for all hazards, including natural disasters, acts of terrorism, and other man-made disasters. The

first Federal Preparedness Report is currently in internal FEMA review and will soon be submitted to Congress.

I understand that the report is close to completion. I understand that FEMA has recently completed an extensive round of data collection that will enhance the content of the report. If confirmed, I will ensure the report is comprehensive and is submitted as quickly as possible.

If confirmed, I will work closely with NPD to ensure that Federal Preparedness Reports are completed in a timely fashion to ensure a Nation prepared.

19. A central way of assessing the efficacy of grants, as well as overall preparedness, is through the use of exercises. Similarly, weaknesses identified in exercises can form the basis for future grant requests. Presumably because of this interrelationship, responsibility for grants and exercises used to be housed in the same office – the previous Office for Grants and Training. However, responsibility for exercises, as well as for determining target capabilities, is now the responsibility of the National Preparedness Directorate, and is not housed in the Office of Grants Programs. Given this new separation, what specific steps do you intend to take to ensure that there is coordination between these two offices and that exercises are designed effectively to advance and assess grant goals?

ANSWER:

I firmly believe that exercises are valuable tools in evaluating performance, identifying shortcomings, and isolating specific corrective actions to improve performance. I believe one of the signature accomplishments of DHS has been the establishment of a National Exercise Program, and development of comprehensive exercise and evaluation guides and guidance for State and local governments. The National Exercise Program is housed within NPD, but serves all FEMA and DHS components, the Federal interagency, and State and local governments. Grant guidance has historically included specific exercise requirements, and if confirmed I will work closely with Deputy Administrator Schrader and the National Integration Center staff to ensure grant programs, activities and services are closely synchronized with exercise programs, including securing feedback from exercise after action reporting to shape future grant priorities and areas of special focus.

Risk Assessment

20. In the past, the Department's methodology for assessing risks faced by states and localities for the purpose of allocating grant funds varied considerably – and often inexplicably – from year to year. For example, a state's population density – a widely accepted factor in assessing terrorism risk – had always been included as part of the Department's risk assessment methodology, but was suddenly deleted from the risk assessment formula in FY2007. The Implementing Recommendations of the 9/11 Commission Act requires the FEMA Administrator to take into account certain

specified risk factors each year in allocating grants under the State Homeland Security Grant Program (SHSGP) and Urban Area Security Initiative (UASI). How do you intend to change FEMA's approach to developing risk assessment methodologies and allocating risk-based funds in light of the law's new requirements?

ANSWER:

DHS will continue to develop its risk analysis to ensure that the Nation's homeland security funding is allocated with maximum effectiveness. Effective risk analysis allows us to make informed judgments about allocation of resources not only to address specific dangers, but also to identify opportunities where key investments can significantly advance our ability to mitigate risks across a wide range of threats and hazards. There is a degree of irreducible uncertainty in any formulation of risk, so expert judgment and experience remain important contributors to final decisions about risk, and its relationship to allocations.

The factors specified in the Implementing Recommendations of the 9/11 Commission Act are essential to effective risk formulation. DHS already incorporates many of these factors into its risk formulations. In FY 2007, DHS simplified, refined, and strengthened the risk analysis formula, putting more weight on risk to people, either through population, or economic variables that represent a population's activities; DHS also made significant strides in communicating how the risk analysis is conducted, what factors are taken into account, their relative weights in the overall formula, and the sources of data. The FY 2007 formulation incorporated familiar, standard practices of the expert risk community and the informed judgments of the intelligence community and other experts. For FY 2008, DHS is fully addressing the specific risk criteria specified in the 9/11 Commission Act, including, for example, the use of Metropolitan Statistical Areas in the Urban Areas Security Initiative risk analysis, the use of population density in the State risk analysis, and the consideration of land and sea borders. DHS is committed to continue refining risk assessment methodologies in accordance with the requirements of the 9/11 Act.

21. The Implementing Recommendations of the 9/11 Commission Act requires that the FEMA Administrator allocate funds for SHSGP and UASI grants in large measure on the basis of the relative threat, vulnerability and consequences from acts of terrorism faced by states and urban areas. Currently, however, it appears that much of the work in assessing the risk to states and urban areas is being done outside of FEMA, in the National Protection and Programs Directorate.

    a. What role do you believe the Office of Grants Program should play in assessing the risk faced by states and localities from terrorism for the purpose of allocating homeland security grants?

    b. If confirmed, how will you, as Assistant Secretary for Grant Programs, ensure the quality and reliability of the data provided to you by NPPD or others outside FEMA?

c. What role will you play in coming up with the risk assessment methodology that will ultimately help determine how a significant portion of the grants administered by the Office of Grant Program are allocated?

ANSWER:

If confirmed as the Assistant Administrator for Grant Programs, I would expect to have primary responsibility, working with the Deputy Administrator for National Preparedness, for determining the architecture for the grant programs within FEMA. I would expect the NPD's subject matter experts to be principal partners with those in the GPD in crafting selection criteria associated with the application review process, and would work closely as well with their counterparts in the National Protection and Programs Directorate (NPPD), Transportation Security Agency (TSA), and the United States Coast Guard (USCG) to do so. I would also expect to be charged with working closely with all these organizations and the Department's Chief Intelligence Officer in the development of risk assessments used to inform grant allocations, guidance and application kits. The assessment of risk is inherently a Department-wide activity, drawing on the specialized expertise of all these organizations to produce the most accurate and comprehensive estimates possible. I am committed to ensuring the process has the required rigor and discipline, that sources and types of data are validated, and that we strike the right balance between transparency and operational security to maintain the integrity and confidence in our risk analysis.

22. Assessing the risk of terrorism is notoriously difficult, as is determining the comparative accuracy of particular risk methodologies.

a. Given the difficulties and uncertainties, what would be your approach to terrorism risk assessment?

b. If a particular risk methodology was proposed to you, how would go about assessing its relative merit and what criteria would you use in determining whether it was appropriate to use in allocating grants to states and urban areas?

ANSWER:

Risk is a conceptual balance between danger and opportunity. Effective risk analysis allows us to make informed judgments about allocation of resources not only to address specific dangers, but also to identify opportunities where key investments can significantly advance our ability to mitigate risks across a wide range of threats and hazards. There is a degree of irreducible uncertainty in any formulation of risk, so expert judgment and experience remain important contributors to final decisions about risk, and its relationship to allocations. I am committed to ensuring the process has the required rigor and discipline, that sources and types of data are validated, and that we strike the right balance between transparency and operational security to

maintain the integrity and confidence in our risk analysis. If confirmed, I would expect to be charged with coordinating with the Deputy Administrator for National Preparedness, the Department's Chief Intelligence Officer, and the National Protection and Programs Directorate, Office of Infrastructure Protection, Transportation Security Administration, and United States Coast Guard to ensure that the risk assessment process has the required rigor and discipline, that sources and types of data are validated, that both the quantitative and qualitative aspects of risk analysis are considered appropriately, and that we strike the right balance between transparency and operational security to maintain the integrity and confidence in our risk analysis.

23. The Implementing Recommendations of the 9/11 Commission Act requires that each year, FEMA submit to Congress a detailed and comprehensive explanation of the risk assessment methodology proposed to be used to allocate grant funds. The explanation is required to be submitted by the earlier of October 31 or 30 days before issuance of grant guidance. Do you anticipate that the explanation and methodology will be submitted to Congress on time as statutorily required?

ANSWER:

The Department is currently finalizing its FY 2008 risk analysis methodology, incorporating factors and criteria specified in the 9/11 Commission Act, and developing the appropriate explanatory materials. If confirmed, I will work closely with the Deputy Administrator for National Preparedness, the Department's Chief Intelligence Officer, and the National Protection and Programs Directorate, Office of Infrastructure Protection, Transportation Security Administration, and United States Coast Guard to ensure that the risk assessment process utilizes a robust, rigorous methodology and draws upon the best available data, and that explanations of the methodology provide the appropriate level of transparency into the process and are made available in a timely fashion.

Integration of Grant Programs

24. The Implementing Recommendations of the 9/11 Commission Act expresses the sense of Congress that "in order to ensure that the Nation is most effectively able to prevent, prepare for, protect against, and respond to all hazards, including natural disasters, acts of terrorism, and other man-made disasters . . . the Department should administer a coherent and coordinated system of both terrorism-focused and all-hazards grants." The Office of Grant Programs is responsible for administering both terrorism-oriented grants, such as SHSGP and UASI grants, as well as all-hazards grants, such as Emergency Management Performance Grants (EMPG) and Interoperable Emergency Communications Grants. What steps do you intend to take to fulfill the sense of Congress and ensure that there is coherent system of grants so as to most effectively prepare for both man-made and natural disasters?

ANSWER:

While each of the preparedness, prevention, and protection programs have historically maintained a specific area of focus, be it terrorism- or natural hazards-oriented, the end result benefit of each program has allowed for a greater baseline level of homeland security overall. Grant program dollars have been and continue to be used in the following areas, most of which can be employed in both terrorism- and natural-hazard scenarios:

- Procurement of equipment in over 21 categories;
- Development of a wide-range of operational and strategic plans;
- Development and conduct of a wide-range of training subjects;
- Development and conduct of a wide-range of exercise scenarios and types; and
- The hiring of personnel who can serve in a variety of capacities, including the strategic and organizational leadership and support capabilities of homeland security; planners; developers of training and exercise materials; and fusion center analysts.

The Department has also historically embraced its relationships with State and local partners and associations in an effort to ensure that the grant programs are fulfilling needs and priorities. Annual conferences and after-action reviews have been hosted with representation from all facets and levels of homeland security in attendance. These gatherings have allowed for a mutual opportunity in providing thoughts, ideas, and recommendations for what has been successful as well as what areas need to be improved upon within the grant programs. The GPD also maintains close relations with other components within the Department and also external to the Department (including DHHS, DoD, DoT, DOE, DoEd, USDA, etc.).

Moreover, PKEMRA clearly spells out the requirement to ensure our grant programs, as well as other preparedness programs, activities and services support the National Preparedness System, including the NPG and national preparedness priorities. The PKEMRA guidance provides strategic coherence for all-hazards national preparedness, and the role of the grant programs in building all-hazards capacity is reflected both in PKEMRA and the Implementing Recommendations of the 9/11 Commission Act. If confirmed, I will ensure grant programs support these requirements and make their critical contributions to accomplishing the vision in the NPG.

Finally, I will continue to employ guidance requirements that direct strategic organization and programmatic coordination take place at both the State and Urban Area levels. More details on these required State and Urban Area structures are detailed in the following question's answer.

25. The Post-Katrina Act gave FEMA the responsibility for administering all DHS grants to state and local governments. Although other components within the Department

appropriately contribute their subject matter expertise – the Transportation Security Administration providing input on transportation grants, the Coast Guard providing its perspective on port security grants – it was deemed important that there be one component, FEMA, which would ultimately oversee all the grants, for at least two reasons. First, this maintains and builds upon the long-standing idea of a "one-stop shop" for grants – a single office, the Office of Grant Programs within FEMA, that state and local governments can contact with questions about any and all grants for which they might be eligible. Second, and perhaps more importantly, it provides one office the ability to look across grant programs to ensure the guidance provided and the requirements imposed are consistent and, most importantly, that the grants awarded work together to foster overall preparedness. A single geographic area may receive SHSGP, UASI, port security, transit security, interoperable communications, EMPG grants and more – and to be most effective those grants need to be allocated and used in a coordinated fashion, to work together to promote preparedness in that area.

a. What is your understanding of the Office of Grant Programs' role in administering the full range of state and local homeland security grants? What is your understanding of what the role of other Departmental components will be in the grants process? In the case of grants that may involve the subject matter expertise of other components, what is your understanding of the division of responsibilities in determining grant allocations among recipients? In developing grant guidance?

ANSWER:

The FY2007 grant program application provided a clear delineation of the division of responsibilities. FEMA has the lead for designing and operating the administrative mechanisms needed to manage DHS' core grant programs. In short, FEMA ensures compliance with all relevant Federal grant management requirements and delivers the appropriate grant management tools, financial controls, audits and program management discipline needed to support the core programs. Effective grant program management entails a partnership within DHS, and Secretary Chertoff has established the boundaries and rules for a seamless partnership.

The GPD will provide a unified, solutions-oriented approach to Federal financial assistance management in support of FEMA's multi-faceted mission, priorities, and customer base. Historically the Department's preparedness, prevention, and protection grant programs have been developed in coordination with sister components and agencies, including the National Protection and Programs Directorate; Customs and Border Patrol; Domestic Nuclear Detection Office; U.S. Coast Guard; Transportation Security Administration; and Chief Medical Officer. FEMA intends to continue employing this relationship in its ownership of homeland security grant programs.

With respect to the determination of grant allocations, the Department's preparedness, prevention, and protection grant awards have either been population-based driven or risk- and effectiveness-based driven. For population-based methodologies, the Department has historically determined allocations in compliance with the USA PATRIOT Act formula, using a base amount of 0.75% of the total allocation for each state (including the District of Columbia and Puerto Rico), and 0.25% of the total allocation for each U.S. Territory, with the balance of funds being distributed on a population-share basis.

For grant programs that have employed a risk- and effectiveness-based methodology, the structure for the risk methodology has been closely coordinated with the Office of Intelligence Analysis (IA) as well as senior leadership within the Department. IA is engaged only in determining the methodology, not the actual grant award amounts. Effectiveness of grantees' proposed Investment Justifications is determined by homeland security peers in an official peer review panel process. As in the case with IA, actual grant award amounts are not determined by peer reviewers. Ultimately, award amounts are determined at the most senior homeland security leadership levels, based upon the results of the risk methodology coupled with the effectiveness scores.

b. If confirmed, how will you ensure that each of the Department's grants in a single geographic area work synergistically to promote preparedness?

ANSWER:

In my observation, the grant programs have guided and encouraged collaboration by, for example, requiring governance bodies to ensure the synergy necessary for an integrated approach to homeland security. In my review of publicly available grant documentation, I was encouraged to see that FY2007 program guidance re-emphasized the importance of creating or utilizing existing governing bodies (such as State Senior Advisory Committees, Urban Area Working Groups, Area Maritime Security Committees, Citizen Corps Councils, and Metropolitan Medical Response System Steering Committees) to act on guidance and coordinate grant resources. The program guidance also encouraged States to examine how they integrate preparedness activities across disciplines, agencies, and levels of government, including local units of government. It directed States to implement a cohesive planning framework to leverage Federal and State resources. It noted that specific attention was required to determine how all available preparedness funding sources could be effectively utilized in a collaborative manner to support the enhancement of capabilities throughout the State. The FY2007 grant cycle also included, for the first time, opportunities for proposing investments that involve multiple States or Urban Areas in support of enhanced regional collaboration. If confirmed, I will strongly support synchronization and synergy to ensure our homeland security resources provide the most return on these critical investments.

Regional Coordination

26. Most of the grants administered by the Office of Grant Programs are awarded to individual states. Yet neither terrorist attacks nor natural disasters respect political boundaries. What steps will you take to promote greater regional coordination and regional preparedness?

ANSWER:

FEMA's Urban Areas Security Initiative promotes regional preparedness investments to high-threat metropolitan areas that often reside in multiple states for the reason that terrorist attacks and natural disasters do not respect political boundaries. In addition, FEMA's state-based homeland security grant programs are purposefully structured to promote regional preparedness within States through the State Strategy and enhancement plan process, as well as by funding state-wide programs that force state-wide collaboration.

An effective coordination of preparedness initiatives must begin as early as possible and, with the co-location of homeland security grant programs at FEMA, the Federal government now has the opportunity to achieve that coordination from the very start of grant administration. FEMA's GPD will administer all of FEMA homeland security grant programs to ensure that they are consistent and integrated. Moreover, FEMA's Regional offices will extend that level of coordination and integration to the field. As a result, State, local, and tribal governments, the private sector, and citizens will have to work together to access most homeland security funding sources with the same Regional offices that understand their needs in the steady-state as well as during disasters. A streamlined grant system administered through FEMA's Regional Office structure will encourage improved coordination among the State Administrative Agencies (SAAs), Emergency Management Authorities, Homeland Security Offices, Urban Areas, and other grant applicants.

27. What role, if any, do you believe FEMA's regional offices should play in grants administration?

ANSWER:

The FEMA Regional structure provides tremendous opportunities to benefit the administration of DHS homeland security grant programs. FEMA's ten Regional Offices are positioned to ensure that the application of grant programs reflect the risks, priorities, and initiatives specific to each Region. Moreover, FEMA can build upon the existing robust relationships present between the Regional offices and their respective State, local, and tribal governments, territories, private sector, and citizens to improve coordination across jurisdictional boundaries.

FEMA is in the process of hiring additional personnel to be located in the FEMA Regional Offices to administer preparedness programs – including Grant Management Specialists. In Fiscal Year 2008, the Regions are anticipated to play a role in most grant program functions and help facilitate regional coordination and information sharing. As additional resources are obtained, an increasing number of grant functions will be performed at the Regions, such as strategic consulting, application processing, and awards.

Grants to Tribes

28. Under the Implementing Recommendations of the 9/11 Commission Act, for the first time Indian tribes will be permitted in some circumstances to apply directly for homeland security grants under the State Homeland Security Grant Program. What do you see as the unique challenges in addressing homeland security on tribal lands, and how do you believe that SHSGP grants can effectively be used to address those challenges?

ANSWER:

Historically, annual DHS appropriations language has included Tribal nations in the definition of local units of government. Thus, Tribal nations have been eligible to receive funds as sub-grantees from the states in which they are located. The 9/11 Act has altered that framework to allow for Tribal nations under certain circumstances to apply for direct funding.

Tribal nations face several unique challenges in addressing homeland security on their lands. For instance, the receipt of Federal funds through these and other grant programs requires a robust programmatic and financial infrastructure to ensure accountability. The application, reporting, and monitoring processes that are associated with the State Homeland Security Program require significant time and personnel commitment from the fiduciary agent charged with implementing the grant. Moreover, the grant program requires that all expenditures be directly linked to a homeland security strategy to ensure that the expenditures (either in the form of planning, training, exercises, or equipment purchases) fit with a broader strategic approach that will bring demonstrable enhancements to preparedness capabilities. That homeland security strategic framework likely does not exist in many Tribal nations, which will require significant front-end effort prior to the expenditure of any grant funds. That complexity has grown in recent years as the Department has shifted more toward risk-based funding to enhance capabilities to prevent, protect against, respond to, and recover from terrorist attacks.

Finally, the successful implementation of SHSGP activities is predicated on cohesive, regional planning and an understanding of shared risks. While in some cases, Tribal nations undoubtedly have strong ties to surrounding communities, to include the unique requirements of homeland security planning, in many cases this regional collaboration may not exist, which creates the potential for duplicative or ineffective

investments.

Grant Funding

29. At the time he signed the Implementing Recommendations of the 9/11 Commission Act on August 3, 2007, President Bush asserted that the bill "authorizes billions of dollars for grants and other programs that are unnecessary or should not be funded at such excessive levels." The President had earlier in the year proposed a budget that, if adopted, would have cut DHS's major homeland security first responders grants by 37%, on top of a 43% cut in those grants since FY2004.

    a. Do you believe that the appropriations authorized for SHSGP, UASI and other homeland security grants in the Implementing Recommendations of the 9/11 Commission Act are excessive? If so, for which specific grants do you believe the authorization levels are excessive?

    ANSWER:

    Including FY07 funding, State and local partners have been awarded nearly $20 billion for homeland security and emergency management efforts. While this funding has already been awarded, some of the dollars are still in the procurement process and have yet to be actually spent. I believe the Administration's budget reflects this fact.

    If confirmed, my objective will be to ensure that grant resources are focused on our Nation's highest risks, and that the enhanced investment processes DHS has developed will be applied to ensure the greatest return on investment to the American public.

    In my prior position as the CEO of a major nonprofit I was responsible for making tough decisions with limited financial resources. Through two budget cycles and on a daily basis I worked with individual stakeholders and multiple cost centers to ensure that those that we were entrusted to provide services to received the best in residential, medical, nutritional and educational benefits.

    b. What do you believe are the funding levels necessary to ensure that we achieve adequate national preparedness?

    ANSWER:

    For FY 2008, the President has requested $1.721 billion in grant funding for State and local responders. I believe that the President's budget is sufficient to continue the excellent progress we have made towards advancing national preparedness in this country. Since September 11, 2001, the Department has provided close to $20 billion dollars in grants to State and local entities to prevent, protect, respond to and recover from incidents or terrorism or other catastrophic events. These

dollars have been invested in critical items related to planning, purchase of equipment, training and exercises. Each year has seen an increasing level of sophistication by our State and local constituents as they work towards developing measurable outcomes for the success of their programs.

c. How will you go about determining what the necessary funding levels are to achieve such preparedness?

ANSWER:

I will work closely with senior leadership of the Department as well as the Administration to develop subsequent funding levels that reflect an appropriate level of investment for these grant programs. This year's State Preparedness Reports, which are the first step in measuring preparedness in a meaningful way, will help to inform decision makers of the gaps in our Nation's preparedness and we will use the grant programs to address those gaps in a deliberative manner.

Accountability

30. The Implementing Recommendations of the 9/11 Commission Act provides for enhanced review and auditing of DHS grants programs. What steps will you take to ensure that these provisions are fully implemented, and that grant funds are being spent properly and effectively?

ANSWER:

GPD is committed to taking the appropriate steps to ensure that grant funds are spent properly and in accordance with existing financial and programmatic guidelines. As such, GPD's Preparedness Officers continually monitor grant implementation, including appropriate and timely obligation and expenditure of grant funds. This office-based monitoring is conducted through quarterly financial status reports, bi-annual progress reports, correspondence, and routine communication with grantees.

It is my understanding that there are established monitoring protocols requiring at least one on-site monitoring visit be conducted each year with the State Administrative Agency (SAA), and once every two years for the Urban Areas Security Initiative (UASI) Working Group. During this visit, Preparedness Officers may conduct interviews with State program implementation staff, review records, review state procedures and guidelines, visit sub grantees, and verify equipment purchases. These protocols also require a review of three items: the review of progress made towards the goals and objectives noted in the State and/or Urban Area Homeland Security Strategies; progress made against the eight National Priorities as noted in the NPG, and progress made against the Investment Justifications submitted with the HSGP application package.

Two additional robust reporting mechanisms, the Initial Strategy Implementation Plan (ISIP) and the Biannual Strategy Implementation Report (BSIR), provide detailed expenditure information by discipline, solution area (such as equipment or training) and project area. These reports require grantees to tie any expenditure of homeland security funds to goals and objectives outlined in their State or Urban Area Homeland Security Strategy.

It is my understanding that the financial side of GPD is currently streamlining its monitoring protocols. If confirmed, I look forward to joining my team in this effort, as financial accountability is a top priority.

As outlined in the steps above, I believe that GPD's monitoring protocols will provide for the enhanced level of review that the 9/11 Act envisions.

31. The Implementing Recommendations of the 9/11 Commission Act authorizes an additional $8 million in each of the next three fiscal years to support enhanced programmatic and financial reviews of prevention and preparedness grants awarded by the Department, although no additional money has yet been appropriated for this purpose. What additional resources do you believe the Office of Grant Programs would need to fully and effectively carry out these responsibilities?

ANSWER:

Although the Implementing Recommendations of the 9/11 Commission Act authorized $8 million for each of the next three fiscal years for enhanced programmatic and fiscal monitoring, no money has yet to be appropriated for this type of activity. Monitoring grants is a requirement, and let me say that I believe a very necessary one. If confirmed, I plan to leverage Regional assets for monitoring and assess additional requirements.

GPD already employs a robust monitoring capability for both administrative and programmatic reviews of HSGP funding. Existing monitoring protocols require at least one formal on-site monitoring visit each year for SAAs, and one visit every two years for each UASI recipient. I will build upon this existing protocol.

32. In addition to oversight over prevention and preparedness grants, it appears the Office of Grant Programs will also oversee auditing and compliance with respect to disaster assistance grants. The problems that have previously arisen in connection with such grants have been well publicized. What additional actions, if any, do you believe should be taken to improve compliance in the area of disaster assistance grants?

ANSWER:

Significant progress has already been made to remedy compliance in the area of disaster assistance grants. FEMA has been proactively implementing more stringent controls programmatically and financially for its suite of disaster programs. New processes and internal controls have been put in place to review, validate and certify eligibility for, disbursement of and receipt of Federal funds. FEMA distributes disaster funds through direct Federal assistance, loans and grants. The six disaster grant programs are: Crisis Counseling Program, Public Assistance, Individual Assistance (Other Needs), Hazard Mitigation Grant Program, Fire Management Assistance Grant Program, and Urban Search and Rescue. These programs are programmatically owned by other FEMA directorates; however, GPD has oversight responsibility for grant management/financial compliance. It is my understanding that the new GPD established a Regional Operations and Business Support Branch with a focus on disaster program oversight.

I also understand that FEMA has been working closely with the Office of Inspector General during disaster operations to identify compliance issues, which allows for immediate and timely corrective actions to be taken. Further, to strengthen oversight, a unified system for tracking audit findings is being implemented. Common audit findings where weaknesses were identified and incorporated into monitoring criteria will be shared across FEMA to ensure future compliance with the requirements.

I support these strengthened efforts, and if confirmed, will continue to evaluate these efforts to ensure strong and effective oversight of disaster programs.

Port Security, Transportation Security and Other Infrastructure Protection Grants

33. In response to a Coast Guard estimate of the cost to provide basic physical security to U.S. ports, Congress has repeatedly authorized and appropriated additional funding for the Port Security Grant Program beyond the Administration's annual budget request. Despite the continued need to improve the basic security measures implemented at U.S. ports post-9/11, DHS has now determined that the Port Security Grant Program should be the primary mechanism for assisting local ports as they implement the requirements of the Transportation Worker Identification Credential (TWIC). This will leave fewer funds available for other security measures, such as hardening perimeter security or for the purchase and deployment of surveillance equipment to improve maritime domain awareness and address a small vessel threat.

    a. Do you believe the Port Security Grant Program is the proper mechanism for providing federal assistance to local ports in order to comply with TWIC regulations?

    ANSWER:

    If confirmed, I will work closely with the U.S. Coast Guard and other DHS components to understand current program status and the appropriate disposition of TWIC requirements. The interests of security and safety are clearly served by adopting an area-wide and fully integrated approach to port security, beginning

with credentialing and access control. If confirmed, I will consult with the Department's subject matter experts to understand the appropriate role of Port Security Grants in contributing to the primary security architecture for the nation's ports.

b. Since the initial Coast Guard estimate for domestic port security was completed prior to the rollout of TWIC, it did not include costs for deploying any equipment or infrastructure which would be required for that program. Do you believe additional funds are therefore necessary?

ANSWER:

If confirmed, I will work closely with the subject matter experts in the Coast Guard and other DHS components to gauge the potential impact on the Port Security Grant Program, on the area-wide security and safety of the nation's ports, and on funding levels.

34. Section 1406 of the Implementing Recommendations of the 9/11 Commission Act requires the Secretary give appropriate consideration to the risks of an entire public transportation system, including the various portions of States into which a system may operate, when awarding grants to a system which operates in multiple States.

a. How will you ensure DHS will give appropriate consideration to the security of all portions of multi-state transit systems?

ANSWER:

It is my understanding that DHS will continue the concept of treating an urban area or multi-state region as a system of systems that has been incorporated into the grant process with the FY2005 establishment of Regional Transit Security Working Groups (RTSWG) in all of the eligible regions. The RTSWG invites representation from the applicable state(s) and urban area(s) and provides an inclusive forum for the development of security projects that benefit the entire region as well as the transit systems individually. DHS will continue to support the RTSWG process within future grant cycles.

b. How can we ensure that some parts of multi-state systems are not overlooked when transportation security grants are awarded?

ANSWER:

As I understand it, DHS will continue the RTSWG format and process in future grant cycles. The further development of these working groups and assimilation into the appropriate Urban Area Working Groups as an active participant will help to ensure that all parts of the systems are included in the planning stages for security projects using Federal transportation security grant funding. DHS will

also review eligibility of transit systems in each region on a periodic basis to ensure appropriate inclusion of systems within the region.

35. The Implementing Recommendation of the 9/11 Commission Act includes State and local law enforcement personnel costs as permissible uses of funds for rail, transit and bus security grants, but caps how much of those grant programs may be used for operational costs in some cases.

a. Do you believe federal transportation security grants programs should fund a portion of State and local personnel costs associated with securing those systems of transportation?

ANSWER:

The Federal security grant programs should fund a portion of State and local personnel costs associated with the increasing need to secure systems of transportation. The lack of effective technology to address specific security measures in the transit environment places the transit systems at a distinct disadvantage in meeting current security requirements. The security of transit agencies has historically been under-funded at the local and regional level.

b. Should the amount of funds available for this purpose be capped and, if so, at what level should they be capped?

ANSWER:

The amount of funds available for personnel costs should continue to be capped. The current cap of 25 % of the regional allocation with an additional 25 % available with a DHS approved waiver is a reasonable level in the current state of technology and security. The cap should be reviewed and revised on a yearly basis taking into account advances in technology and other sources of funding available to the transit industry. This cap reflects the differing security needs that exist within the Nation's largest urban regions.

c. What other limitations, if any, should there be?

ANSWER:

Additional limitation on the use of Federal security grant program funds for personnel costs should include:

- Continuing the 50% match requirement;
- Eligibility for funds based on relative risk;
- More robust safeguard measures in regard to supplanting; and
- Use of funds should be limited until training of personnel has reached an established baseline.

Interoperable Communications Grants

36. Congress recently established the Interoperable Emergency Communications Grant Program, which will be administered by FEMA, consistent with guidance established by the Office of Emergency Communications.

    a. DHS is currently coordinating with the Department of Commerce to implement the Public Safety Interoperable Communications (PSIC) grant program, which is a one-time $1 billion program. How will you ensure that grants awarded under the new interoperability grant program build upon, and do not duplicate, interoperability initiatives that are funded under the PSIC program?

    ANSWER:

    Per the published guidance, a requirement of the PSIC grant programs is for each grantee to submit investment justifications to support their interoperable communication projects. The review of these investment justifications will be conducted concurrently with the review of Statewide Communication Interoperability Plans (SCIP) and in coordination with the Office of Emergency Communications (OEC). In developing the program guidance for the new interoperability grant program, OEC and FEMA will leverage the existing processes and plans to ensure that grantees build upon the existing initiatives and infrastructure. As I understand it, the development of SCIP for each State will provide OEC and FEMA a greater understanding of the gaps and needs for each State. This will help to prevent duplication and ensure that Federal grant dollars for interoperability are maximized.

    b. How will you ensure that grants awarded under the new interoperability grant program do not duplicate communications-related initiatives that are funded through other DHS grants?

    ANSWER:

    As discussed above, the development of SCIP for each State will provide DHS with a greater understanding of the gaps and needs for each State. This will help to prevent duplication and ensure that Federal grant dollars for interoperability are maximized.

    c. DHS is authorized to award grants after the Department submits to Congress the National Emergency Communications plan, due by April 2008. What steps will you take in advance of that date to establish guidelines for states and procedures for applications, so that the program will be up and running by April 2008?

ANSWER:

To ensure that guidelines for States and procedures for applications are in place by April 2008, FEMA will continue to work closely with OEC in developing the new interoperability grant program. In addition, DHS will leverage the guidance that has already been developed for the PSIC other Homeland Security grant programs to ensure that the new interoperability grant program is consistent with existing DHS policies and program guidance.

Metropolitan Medical Response System

37. The grant program for the Metropolitan Medical Response System (MMRS) offers DHS the opportunity to promote public health preparedness at the local level. It is suggested that the program suffers however from the lack of a clear mission coordinated across the 124 jurisdictions and a system of measures and metrics by which to evaluate the capabilities they have attained.

    a. What steps will you take to leverage this program to address local preparedness planning?

    ANSWER:

    The MMRS Program was created in 1996, in response to the Tokyo mass transit Sarin gas attack by Aum Shinrikyo and the domestic terrorist bombing of the Alfred P. Murrah Building in Oklahoma City, both having occurred in 1995.

    The MMRS program assists highly populated jurisdictions to develop plans, conduct training and exercises, and acquire pharmaceuticals and personal protective equipment, to achieve the enhanced capability necessary to respond to a mass casualty event caused by a WMD terrorist act. This assistance supports the jurisdictions' activities to increase their response capabilities during the first hours crucial to lifesaving and population protection, with their own resources, until significant external assistance can arrive.

    Gaining these capabilities also increases the preparedness of the jurisdictions for a mass casualty event caused by an incident involving hazardous materials, an epidemic disease outbreak, or a natural disaster. MMRS fosters an integrated, coordinated approach to medical response planning and operations, as well as medical incident management at the local level. It is my understanding that MMRS is already included as part of the suite of grants offered to our state and local partners as part of the Homeland Security Grant Program.

    b. Do you intend to work with member jurisdictions to identify a core mission statement, minimal mission capabilities, a system of measures and metrics by which to gauge their performance, and to develop a five year outlook for the program?

ANSWER:

It is my understanding that there is a strong relationship with the MMRS jurisdictions and FEMA. There have been many formal and informal discussions with the MMRS community to find ways to better serve them as both in the context of both a grant program and a functional component. They have indicated that the relationships and response capabilities have improved across the Nation as a result of the MMRS program. Simultaneously, these leaders agree that for the program to continue in the future, program objectives must be clearly defined and measurable and that accountability is paramount. Some key steps that are under consideration for the future of the MMRS program include the following:

(1) Limit the scope of the program to focus on one primary and a very few secondary objectives. The MMRS community has expressed that too many targets for activity were problematic. The program's primary program focus area should be "pre-hospital care and emergency treatment of patients" and the secondary areas should support the ability of the jurisdiction to effectively respond to a mass casualty event regardless of the triggering event.

(2) Develop better metrics to clearly define performance expectations for jurisdictions and enhance the ability of the national office at FEMA / DHS to ensure accountability and the best use of the funds. The national office should regularly collect and analyze the jurisdictional data resulting from the new metrics, and use this information to support effective programs, assist struggling programs and eliminate programs that are not attempting to meet the program measures.

In addition, work continues with the local leaders of the MMRS program to keep the presence of the local element of the program intact for which the program was founded and built upon. It is my understanding that this is done within the current grant structure where the State also plays a key role in placing MMRS as a high priority in terms of strategic planning and allocations of resources. There is expected to be significant flexibility in the upcoming grant cycle to support this much needed element of local planning for the MMRS program as I believe that MMRS has been a valuable tool for establishing and encouraging organizational relationships among health care, medical, and first responder communities.

Management

38. What is your approach to managing staff, and how has it developed in your previous management experiences?

ANSWER:

My staff management approach can best be described as an inclusive leadership process. I feel and have demonstrated in the past that by developing open and mutual respect staff relationships creates a successful environment. I believe that strong mentorship is also a key component to my approach. In my past management experiences I have been called upon to not only lead an organization but also to develop strong leadership teams that would, and have, survived my departure.

I have had the privilege to manage in a number of capacities that span from leading small focused teams to running an 1100 person organization as Chief Executive Officer. I also have served in a variety of leadership positions in the National Guard and Reserve to include being the Non-Commissioned Officer in Charge of an intelligence unit and being the Chief of Targets as a Commissioned Officer.

39. What actions in your past executive experiences demonstrate your style and approach in the area of labor-management relations?

ANSWER:

In my role as Chief Executive at the National Children's Center, I inherited from my predecessor a failed union organizing effort that resulted in eleven election objections and two unfair labor practices filed by Service Employees International Union (SEIU) against the previous management team. Working with the union and the National Labor Relations Board (NLRB), I settled the unfair labor practices to satisfaction of the union and allowed without protest for a new election to take place thus eliminating the eleven election objections. The resulting election led to a successful effort by the union in a fair process to represent the employees of the National Children's Center. Throughout my time as the Chief Executive I led the management negotiating team working towards a mutually agreed upon contract between management and their employee representatives.

Use of Contract Personnel

40. How many individuals work for the Office of Grant Programs? Please include all individuals to whom an identification badge has been issued. Of those issued identification badges, how many are contractors?

ANSWER:

It is my understanding that as of October 15, 2007, there are currently 215 individuals who work for the Grant Programs Directorate. Of those 215 individuals, 90 are contractors and 125 are Federal employees.

41. Excluding funds that were distributed to grant recipients, what was the budget in FY2007 for the Office of Grant Programs? Of this money, please indicate how much was spent on:

a. all services contracts;

b. contracts for professional and management support;

c. salaries and benefits for government employees.

ANSWER:

As I understand it, FY 2007 expenditures for all service contracts totaled close to $21 million. Of that amount, $1.65 million was spent on contracts for professional and support services. Salaries and benefits for government employees in FY 2007 totaled close to $5 million.

42. Do you believe that the Office of Grant Programs is currently making appropriate use of contractors, or that it is over- or under-utilizing contractors? If confirmed, what factors would you consider in determining whether or not to use contractors for particular professional and management support services in the Office of Grant Programs, and how would you weigh those factors?

ANSWER:

Based on my current knowledge of the GPD's operations, I believe that the Directorate is making appropriate use of its contractor staff to perform services that are not inherently governmental in nature. If confirmed, I will closely review the use of contractor services to ensure that professional and management support contracts are not utilized to perform inherently governmental functions and that agency officials retain control over and remain accountable for policy and program decisions.

Miscellaneous

43. Did the Department contract with a public relations or other outside firm to manage the public relations surrounding the announcement of grant awards under the FY2007 Homeland Security Grant Program? If so, how much did DHS spend for this purpose?

ANSWER:

To my knowledge, the Department did not contract with a public relations or other outside firm to manage public relations surrounding the announcement of FY 2007 Homeland Security Grant Program awards. These functions were performed by a core cadre of career civil service personnel with programmatic and public affairs expertise as part of their day-to-day functions.

44. Do you believe that it is a good use of taxpayer funds to hire a firm for this purpose? If confirmed, do you intend to hire a public relations firm to handle grants announcements?

ANSWER:

I will confer with FEMA leadership on this matter. It is my understanding that the Department does not believe that it is a good use of taxpayer funds to contract with an outside public relations firm for grant announcements. Although the announcements each year can become politicized by third parties who point to increases and decreases in allocations, the Department believes that its staff is best positioned to explain and answer questions about the analytical process used to determine final allocations, not an outside public relations firm.

V. Relations with Congress

45. Do you agree, without reservation, to respond to any reasonable summons to appear and testify before any duly constituted committee of the Congress if you are confirmed?

ANSWER:

Yes.

46. Do you agree, without reservation, to reply to any reasonable request for information from any duly constituted committee of the Congress if you are confirmed?

ANSWER:

Yes.

VI. Assistance

47. Are these answers your own? Have you consulted with DHS or any interested parties? If so, please indicate which entities.

ANSWER:

I have received assistance from FEMA with some of the policy questions. Some of the questions are at a level of detail that I would not have had the opportunity to gain the requisite internal knowledge to make a reasoned judgment. Therefore, I could not fully answer the questions without some input from the individuals involved.

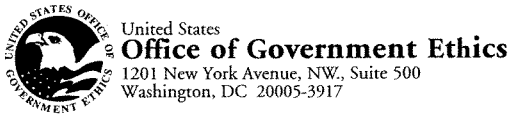
AFFIDAVIT

I, Wiley Ross Ashley III, being duly sworn, hereby state that I have read and signed the foregoing Statement on Pre-hearing Questions and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

Subscribed and sworn before me this 30th day of October, 2007.

Notary Public

Michelle D. Parrish
Notary Public, District of Columbia
My Commission Expires 11-14-2007



July 12, 2007

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510-6250

Dear Mr. Chairman:

In accordance with the Ethics in Government Act of 1978, I enclose a copy of the financial disclosure report filed by Wiley R. Ashley, III, who has been nominated by President Bush for the position of Assistant Administrator for Grant Programs, Federal Emergency Management Agency, Department of Homeland Security.

We have reviewed the report and have also obtained advice from the Department of Homeland Security concerning any possible conflict in light of its functions and the nominee's proposed duties. Also enclosed is a letter dated July 3, 2007, from Mr. Ashley to the agency's ethics official, outlining the steps Mr. Ashley will take to avoid conflicts of interest. Unless a specific date has been agreed to, the nominee must fully comply within three months of his confirmation date with any action he agreed to take in his ethics agreement.

Based thereon, we believe that Mr. Ashley is in compliance with applicable laws and regulations governing conflicts of interest.

Sincerely,

Robert I. Cusick
Director

Enclosures

OGE - 106
August 1992

Senator Daniel K. Akaka
Additional Questions for the Record
Nomination Hearing of W. Ross Ashley, III
November 9, 2007

1. There are concerns about the length of time DHS is taking to execute Homeland Security Grants. Right now, it takes roughly 9 to 10 months from the time the grant guidance is announced to the time the funds are obligated. By the end of that period, most state and local recipients are busy preparing for the next grant period, leaving little time to work on assessments and strategies for the next cycle. If confirmed, what would you do to shorten that time period so that state and local governments could better prepare for the next grant cycle?

   It is my understanding that FEMA's Grant Programs Directorate (GPD) works very hard to ensure that states have sufficient time to prepare the application for Homeland Security Grant Program (HSGP) funding, and to do the deliberative planning work that is necessary to identify gaps in capability across an entire State. If confirmed, I will work to ensure that we work within the statutory timelines. For example, last year, the Department had 45 days to make the application available to states; 90 days for the states to apply for the funding, and 90 days for the program office to act upon those applications. It is understandable that states may find it difficult to accomplish the detailed planning work during these timelines, but we want to make sure that we are operating within the statutory guidance.

   I am committed to finding ways to shorten some of the review time allotted to our review process in order to move the applications into the financial award process sooner while still ensuring that grant funding supports sound, well-planned investments.

2. The Public Safety Interoperable Communications Grants issued by the Department of Commerce in partnership with DHS can be confusing for state and local government applicants. It is not clear who takes the lead in the execution of the program and grant management. Right now, the grant applications are reviewed and approved by Commerce, but issued by DHS. If confirmed, what steps would you take to clarify this grant program and its implementation?

   The Public Safety Interoperable Communications (PSIC) Grant program was authorized under the Digital Television Transition and Public Safety Act of 2005 and Section 3006 of the Deficit Reduction Act of 2005, Pub. L. 109-171 which authorized the National Telecommunications Information Administration (NTIA) of the Department of Commerce (DOC) to establish and implement this program in consultation with the Department of Homeland Security (DHS). This public law clearly demonstrates that NTIA is the lead on the execution of the PSIC program. Memorandums of Understanding (MOU) between the Department of Commerce and the Department of Homeland Security outline that DHS's role is to assist in the administration of this program. Specifically these MOUs state that DHS would

publicize, make the awards, and monitor the grantees; however, the approval of the actual awards lies with the DOC.

It is my understanding that the GPD has taken action to notify their grantees regarding these MOUs and the responsibilities of both DOC and DHS. GPD has included this language in the grant guidance and the Preparedness Officers are also working closely with their states to ensure that they understand the guidelines and can proceed accordingly. GPD has also established a single email address for all questions to be addressed and is working very closely with NTIA to ensure that the same information is being provided by both agencies. NTIA has issued a Fact Sheet that describes the responsibilities of both DOC and DHS according to the MOUs and hosted workshops throughout the country in September with DHS participation to explain the process and answer any questions that arose. NTIA also has a robust website that includes all of this information and continues to update it with all communications that are sent by DHS to their grantees.

If I am confirmed, and find that confusion continues regarding this program, I will meet with both GPD and NTIA staff to determine ways that we can improve upon this process for our grantees.

3. The performance period for the Public Safety Interoperable Communications Grant ends on September 30, 2010. However, this deadline does not allow adequate time for states to begin technology procurement and for suppliers to meet the deadlines. Can you tell me if DHS and Commerce are planning to extend the performance period for this grant program and if not, why not?

The grant period of performance deadline of September 30, 2010 is mandated by section 3006 of the Deficit Reduction Act of 2005, Pub. L. No. 109-171, and there does not appear to be a provision that would allow for an extension of the performance period. Therefore, there are no current plans to extend the performance period. DOC, ultimately, is the lead on this grant program and, if authorized, would have final approval on whether or not grant extensions would be provided.

Senator Susan M. Collins
Additional Questions for the Record
Nomination Hearing of W. Ross Ashley, III
November 9, 2007

1. The Post-Katrina Emergency Management Reform Act of 2006 was the result of this Committee's investigation into the failed response to Hurricane Katrina. One of our principal initiatives was to rejoin the preparedness and response functions within a stronger and more robust Federal Emergency Management Agency. This included moving the former office of Grants and Training into FEMA. The Department of Homeland Security has chosen to divide the grant functions between the FEMA National Preparedness Directorate, headed by Dennis Schrader, and the Grant Programs Directorate, the position for which you are before us now. What is your understanding of your grants-related responsibilities as compared to those of the National Preparedness Directorate at FEMA?

The missions and functions of the Grant Programs Directorate (GPD) and the National Preparedness Directorate (NPD) are inextricably intertwined, thus requiring concerted and ongoing coordination between the personnel that make up these organizations. Effectively, the grant programs that are part of the GPD portfolio are a key vehicle through which the national preparedness initiatives designed through NPD can be implemented at the State and local level. NPD activities cannot effectively be achieved without leveraging the grants managed through GPD; and GPD programs require the strategic input from NPD on national preparedness priorities to focus each grant program.

GPD is responsible for developing, implementing, and monitoring a broad portfolio of preparedness grant programs that cut across prevention, protection, response, and recovery capabilities. This includes (but is not limited to) such programs as the Homeland Security Grant Program, the Infrastructure Protection Program, and the Emergency Management Performance Grant program. GPD staff build the guidance that governs these grant programs and track performance throughout the life-cycle of the grants from both a programmatic and financial standpoint. Additionally, if confirmed, I will oversee the Grant Development and Administration Division of GPD, which will be responsible for the allocation process.

If confirmed, I would expect to have the lead for building the grant processes and products and executing the programs to ensure they support the national preparedness requirements identified in the National Preparedness Guidelines, the Post Katrina Emergency Management Reform and 9/11 Acts, and meet the needs of our grant recipients. If confirmed, I look forward to working closely with the Administrator and Deputy Administrators to support our national homeland security and related strategies, and commit to working closely with our partners in the Transportation Security Agency

(TSA) and the United States Coast Guard (USCG). I will closely coordinate with these key partners throughout program life cycles to ensure grant programs, grant management tools, financial controls, audits and program management fully support achieving the vision of the National Preparedness Guidelines.

NPD is responsible for building the national preparedness policy and doctrinal framework. This includes a range of activities including training, exercises, incident management systems, national assessments, capability-based technical assistance, and the overarching preparedness policy considerations that guide these initiatives. NPD staff are responsible for designing common approaches to achieving and measuring national preparedness.

I plan to work closely with all Directorates within FEMA and with external partners to align our respective roles and to ensure our stakeholders are served by programs that support FEMA's multi-faceted mission, priorities and customer base.

2. If confirmed, you will have programmatic responsibility for 17 grant programs and financial management responsibility for another 31 FEMA grant programs. These grants span the entire gamut of homeland security and emergency management: including prevention, preparedness, response, recovery, and mitigation. I am encouraged by your financial management experience. In the answers to your policy questionnaire, however, you noted that you have never administered a grant program as an employee of the Federal or a State government. How has your private sector experience prepared you for the challenge that lies ahead at FEMA?

I believe a number of private sector experiences have prepared me for the position for which I have been nominated and, if confirmed, will enable me to succeed. First, as a corporate partner with State and local first responders I have had the opportunity to work on grant programs at the grass-roots level. I believe these experiences working across the country will help further bring the end-user perspective to the overall grants process.

Second, as the Chief Executive Officer of the National Children's Center (NCC) I was charged with managing a diverse set of funding streams that cut across State, local and federal agencies. Not only were the individual funding streams from multiple levels of government, they were also cross-functional touching all aspects of the lives of the people we were entrusted to provide care for. NCC received funding to provide educational, recreational, residential, day services, nutritional, medical and a variety of other services. In many cases these funds were from different agencies within a single governmental entity. As I am sure you are aware, individual government

funding mechanisms include unique financial and compliance reporting to ensure outcomes are being met and that funds are being used appropriately. I believe the experiences afforded me as the CEO of NCC have prepared me to assist in grant efforts to provide superior one stop shopping for our State and local partners.

3. In your staff interview, you noted that solid financial management includes ensuring that Americans are receiving the best return on investment possible. I agree that we should take a capabilities-based approach in allocating grant funding to ensure that every area of the country has a baseline level of preparedness. It is also critical for the Federal government to measure how taxpayer dollars are affecting change. How will you ensure our future investments will result in increased levels of prevention and preparedness?

   I believe an end-to-end capabilities-based planning system needs to start by further measuring the investments already made. To date, this Congress and the administration have provided nearly $20 billion in homeland security funding to our State and local partners. Taking into account acquisition and grant cycles, much of this funding is just beginning to provide homeland security capabilities. If confirmed, I will work with our State and local partners and with the National Preparedness Directorate to further capture the impacts these investments have made in the National Preparedness Report submitted annually as required by the 9/11 Act.

   Additionally, the 9/11 Act provides a robust reporting requirement for States to conduct Initial Strategy Implementation Plans (ISIP) and Biannual Strategy Implementation Reports (BSIR). If confirmed, I will fully support the States efforts with these reports and ensure that investments are tied to specific and measurable capabilities. Further, as envisioned in the 9/11 Act, I will work with all components of DHS and external partners to ensure that capability-based planning is cross functional and includes all homeland security investments regardless of the individual grant program.

   Early in my career I worked as a contract analyst with the Department of Defense conducting cost to capability analyses of existing and proposed force structures. During the period I was there, the Department moved from a Soviet-era threat model to a new Defense Planning Guidance focusing on major regional contingencies. If confirmed, I will work with the National Preparedness Directorate to continue the development of an all-hazard capabilities-based planning system, and to ensure that grant investments and outcome measures are included in this process.

4. One of the historical concerns with the homeland security grant programs that State and local first responders have expressed is the lack of continuity and consistency year to year in the grant guidance and risk methodology. The Implementing Recommendations of the 9-11 Commission Act, authored by

Senator Lieberman and me this year, codifies for the first time the State Homeland Security Grant Program and Urban Area Security Initiative and enumerates specific risk factors the Department must consider in making allocation decisions. Our goal is to make it easier for States to plan for multi-year initiatives. What efforts will you undertake to ensure the risk allocation methodology and grant application process is consistent and familiar from year-to-year?

I understand and share your concerns about the challenges that major changes in grant processes pose for states and local jurisdictions. If confirmed, I will work to ensure that the risk formula remains as stable as possible from year to year and reflects the guidance that we have received from Congress in the 9/11 Act. My understanding is that the risk formula was simplified in FY 2007 to enhance transparency and reliability and that those changes were well received. Thus, I would hope to build on that success if confirmed. Moreover, I also understand that the application process changed in FY 2006, with the introduction of Investment Justifications for key programs such as the Homeland Security Grant Program. If confirmed, I would look to continue this process for future years to ensure stability and demonstrate support for the critical planning processes that drive this effort at the State and local levels.

5. It is my understanding that of the 215 individuals that currently work for the Grant Programs Directorate, 90 are contractors and 125 are Federal employees. Therefore 42 percent of your staff is made up of contract personnel. In addition, you noted in your staff interview that at the start of 2008 you will have 26 open positions for federal employees. What will be your approach, if confirmed, to managing staff and determining whether the Grant Programs Directorate contains an appropriate balance of contractor and federal personnel?

Actually there are 166 full-time federal employees within the Grant Programs Directorate. This 166 is made up of 150 legacy G&T employees and 16 legacy FEMA employees. The remaining 75 of the 225 legacy G&T employees were retained by NPD. While most of the legacy contractors from G&T (90) are working to support GPD, some are supporting NPD.

If confirmed, I will closely review the use of contractor services to ensure that professional and management support contracts are not utilized to perform inherently governmental functions and that agency officials retain control over and remain accountable for policy and program decisions.

○