

NOMINATION OF HON. RAND BEERS

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

OF THE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

NOMINATION OF HON. RAND BEERS TO BE UNDER SECRETARY, U.S.
DEPARTMENT OF HOMELAND SECURITY

JUNE 2, 2009

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

51-780 PDF

WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office,
<http://bookstore.gpo.gov>. For more information, contact the GPO Customer Contact Center,
U.S. Government Printing Office. Phone 202-512-1800, or 866-512-1800 (toll-free). E-mail, gpo@custhelp.com.

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

CLAIRE McCASKILL, Missouri

JON TESTER, Montana

ROLAND W. BURRIS, Illinois

MICHAEL F. BENNET, Colorado

SUSAN M. COLLINS, Maine

TOM COBURN, Oklahoma

JOHN McCain, Arizona

GEORGE V. VOINOVICH, Ohio

JOHN ENSIGN, Nevada

LINDSEY GRAHAM, South Carolina

MICHAEL L. ALEXANDER, *Staff Director*

JEFFREY E. GREENE, *Counsel*

KRISTINE V. LAM, *Professional Staff Member*

DEBORAH P. PARKINSON, *Professional Staff Member*

BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*

ROBERT L. STRAYER, *Minority Director for Homeland Security Affairs*

JENNIFER L. TARR, *Minority Counsel*

TRINA DRIESSNACK TYRER, *Chief Clerk*

PATRICIA R. HOGAN, *Publications Clerk and GPO Detailee*

LAURA W. KILBRIDE, *Hearing Clerk*

CONTENTS

| | |
|-------------------------|------|
| Opening statements: | Page |
| Senator Lieberman | 1 |
| Senator Collins | 2 |
| Senator Akaka | 12 |
| Senator Burris | 14 |
| Senator Voinovich | 15 |
| Prepared statements: | |
| Senator Lieberman | 25 |
| Senator Collins | 27 |

WITNESSES

TUESDAY, JUNE 2, 2009

| | |
|---|---|
| General John A. Gordon, U.S. Air Force, Retired | 3 |
| Hon. Rand Beers to be Under Secretary, U.S. Department of Homeland Security | 5 |

ALPHABETICAL LIST OF WITNESSES

| | |
|--|-----|
| Beers, Hon. Rand: | |
| Testimony | 5 |
| Prepared statement | 28 |
| Biographical and financial information | 33 |
| Responses to pre-hearing questions | 44 |
| Letter from the Office of Government Ethics with an attachment | 94 |
| Responses to post-hearing questions for the Record | 96 |
| Letter of Support from Hon. Michael Chertoff | 100 |
| Gordon, General John A.: | |
| Testimony | 3 |

NOMINATION OF HON. RAND BEERS

TUESDAY, JUNE 2, 2009

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

The Committee met, pursuant to notice, at 2:35 p.m., in room SD-342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Akaka, Burris, Collins, and Voinovich.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good afternoon and thanks to all of you for coming to this hearing today for the nomination of Rand Beers to be the Under Secretary for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security (DHS).

Rand Beers is a highly qualified nominee with a record of more than 30 years of public service, dating back to his service as a Marine in Vietnam. He has served in Democratic and Republican Administrations, working as the Senior Director for Combating Terrorism at the National Security Council (NSC) during the Administration of President George W. Bush, as Assistant Secretary of State for International Narcotics and Law Enforcement Affairs during the Clinton Administration, and as Director of Counterterrorism and Counternarcotics at the NSC during the Administration of President George Herbert Walker Bush.

More recently, Mr. Beers played a key role in the transition at the Department of Homeland Security from the Bush to the Obama Administrations, which by all accounts was about as good as a transition can possibly be, and since then has been a chief counselor to Secretary Napolitano.

If confirmed, Mr. Beers will be required to apply this wealth of experience to harness and provide vision for the National Protection and Programs Directorate, which includes quite a wide variety of responsibilities, including cyber security, infrastructure protection, foreign traveler screening, and emergency communications. The President's fiscal year 2010 budget proposes to expand this Directorate further by moving the Federal Protective Service (FPS) into it.

Let me just talk about a few of the areas that I hope and I know will be priorities, if confirmed. Cyber security is clearly one of those. The threat of cyber attacks is an urgent national security,

(1)

homeland security challenge, as we know. Last week, President Obama announced the results of the 60-day review of cyber security policy and government structures. I am grateful for the President's focus on this issue and particularly reassured that, as the President sees it, the Department of Homeland Security has a central role to play in any government-wide cyber security strategy, and the NPPD is the part of the Department that will lead its efforts in that regard. I look forward to hearing what Mr. Beers thinks the Department's role should be and how he will ensure that DHS has the necessary tools to perform the job.

NPPD's critical infrastructure responsibilities are equally challenging because the majority of the Nation's critical infrastructure—our energy, communications, and transportation networks, all potential targets of terrorism—are owned and operated by the private sector. The Department must work closely with the private sector to ascertain that the appropriate security measures are being taken. The lesson from Mumbai, London, and Madrid is that terrorists will seek out soft targets, such as hotels, shopping malls, and inner-city transit lines, so we must accelerate our efforts to harden those targets.

NPPD also plays a critical role in our Nation's security through the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, which requires foreign nationals to undergo biometric screening as they enter the country. The 9/11 Commission concluded that three of the September 11, 2001, hijackers had overstayed their U.S. visas and concluded that requiring biometric exit screening was vital to homeland security. In fact, if we had implemented a biometric system to detect overstays prior to September 11, 2001, there is some reason to believe that we could have prevented the attacks of September 11, 2001. I am very concerned that almost 8 years later, despite the clear need for a viable biometric exit system, we still do not have such a workable system in place. The Committee will continue to work with the Department of Homeland Security to ensure that a secure system is expeditiously deployed, of course, at the Nation's airports, and I look forward to discussing that with Mr. Beers today.

Many other challenges face the NPPD, including the future of our chemical security regulation system, the Directorate's challenge in hiring and retaining qualified staff, and the overdependence, as I see it, on contractors to do what otherwise might be considered inherently governmental work. I look forward to working closely with the new Under Secretary to reauthorize and strengthen the Department's Chemical Facility Anti-Terrorism Standards (CFATS), the chemical security site program.

So, bottom line, Rand Beers is a very experienced public servant. If confirmed, he will need all that experience to be put to use as the Director of the NPPD to protect our homeland security.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman. I join the Chairman in welcoming Rand Beers as the nominee today. As the Chairman has indicated, the scope and importance of the NPPD's responsibilities are daunting. The Directorate is charged with ensuring suc-

successful implementation of the chemical facility security program that was authorized in 2006 due to the work of this Committee. This program is one that needs to be reauthorized this year. It also is charged with assessing the risk to our Nation's critical infrastructure, managing voluntary private sector coordination programs to achieve the goals of the National Infrastructure Protection Plan, leading the Department's effort to protect our Nation against improvised explosive devices and working to combat terrorists' use of such explosives in the United States, and protecting the Nation's cyber networks.

The Chairman and I have focused a great deal on that last responsibility, cyber security. It is both critical and complex. The complexity arises not just from the technical nature of the issue, but from the disjointed approach that the Federal Government has taken. In the course of the coming months, cyber security responsibilities across the Federal Government will be the subject of much debate as we consider the Administration's plan and alternative legislative proposals to strengthen our cyber security efforts.

DHS's relationships with the critical infrastructure sectors that both provide for and rely on information technology services will remain invaluable in ensuring a coordinated defense against cyber attacks. I look forward to hearing from Mr. Beers about how, if confirmed, his management of DHS's cyber security efforts will be affected by the White House's new cyber security initiative.

NPPD also manages programs that benefit components across the Department, including, as the Chairman has indicated, the US-VISIT program that screens the biometrics collected from visitors to the United States against immigration and criminal databases. US-VISIT has been struggling for years with implementing a solution to collect biometric information on foreign travelers departing the country, a responsibility that is required by law but has not been fully realized.

Should Mr. Beers be confirmed, these are just some of the critical challenges that are awaiting his leadership and considerable expertise. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins.

I would like to welcome retired General John Gordon of the U.S. Air Force, who is here to introduce our nominee. We are honored to have you take the time to be here for that purpose, and I call on you at this time.

TESTIMONY OF GENERAL JOHN A. GORDON, U.S. AIR FORCE, RETIRED

General GORDON. Thank you, Chairman Lieberman, Senator Collins. Good afternoon. I am a retired Air Force officer and a former Deputy Director of Central Intelligence, a former Secretary of Energy, a former Homeland Security advisor, and so I now am a rather interested observer of the national security and homeland security scene without a lot of responsibilities, and limited responsibilities. But today, I have the most pleasant responsibility I have had in a while, which is to introduce my friend and my colleague, Rand Beers, to the Committee as you consider his nomination to be Under Secretary of Homeland Security.

To cut to the chase, I know of no individual who is better qualified nor anyone more suited to take on the vital task of protection of America's critical infrastructure, as you both have said, the central responsibility of this position. Nor in my book is anyone more suited to be a member of Secretary Napolitano's leadership team. I offer my unqualified and total support for his confirmation.

Now, to be entirely transparent and with full disclosure, Mr. Beers is a close friend and a longtime professional colleague. We have worked together in the State Department and in the White House for several Presidents, and even so, I do not believe that I suffer from any lack of objectivity in considering his suitability and qualifications for this vital position.

First, and I do rate this first, Mr. Beers is a patriot. He has committed his entire working life to the security of our Nation, beginning as a Marine officer and a rifle company commander in Vietnam, where he served 4 years. Virtually his entire career since then has been in government, largely at the State Department and the White House, and he always found his true reward in the service he gave to our Nation. He is the very model of an American committed to good government, willing to give his time, talent, and energy toward that end.

Mr. Beers is a man of integrity. He can always be counted on to do the right thing, to give his objective and well-considered advice.

Mr. Beers is proven under fire, and I refer not only to his combat experience in Vietnam, but his ability to keep his head and work calmly and effectively through some of the toughest national security and foreign policy situations, and he experienced many of these literal crises as he served in senior positions in peacekeeping, counterterrorism, counternarcotics, intelligence, and Middle East policy.

These items all help define the character of the man, but can he actually do the job? Yes, I am certain he can. Mr. Beers is certainly among the most experienced if not the most experienced candidate for a senior position in Homeland Security. As mentioned already, he has had huge responsibilities in counterterrorism, counternarcotics, political and military affairs, peacekeeping and intelligence, continuously since he joined the Foreign Service in 1971. As you mentioned, Mr. Chairman, he served four Presidents in the National Security Council.

Most recently, Mr. Beers has had the opportunity, I think, to reflect a bit about his experiences and about how the complex issues of national and homeland security all fit together, or at least how they should fit together. For several years, he was President of National Security Network, an organization that he founded to bring together experts seeking to foster discussion of progressive national security ideas. At the same time, he was an adjunct professor at the Kennedy School of Government at Harvard. My sense is that this time of reflection, observation, and teaching has given him a new and broader perspective of the national homeland security, along with a renewed commitment to the urgent task ahead, as well as a deeper appreciation of the long-term strategic goals we must achieve.

If confirmed, we can expect Mr. Beers to immediately be effective with no spin-up time needed. He co-led the transition team, as you

mentioned, Mr. Chairman, at the Department for the incoming administration where he really looked into every aspect of the new and still evolving Department. And today, he serves as counselor to Secretary Napolitano, advising her on the full breadth of the Secretary's mission. I suspect he has identified no shortage of issues worthy of his time and effort, and I commend the list that both of you put forward, headed in many ways by cyber security in addition to the more standard infrastructure protection items.

Mr. Chairman, as I mentioned at the outset, I am not an entirely disinterested observer in this nomination before the Committee today. The Department needs the very best leadership and the full commitment of true professionals as it comes of age and reaches its full stride in what are still very dangerous times, and the country needs the very best to take on these tough jobs. Rand Beers is one of the very best, and I respectfully commend him to the Committee to become Under Secretary of Homeland Security. Thank you.

Chairman LIEBERMAN. Thanks very much, General Gordon. We honor you as a former advisor here. The statement was a very strong one on Rand Beers' behalf, and we thank you for your service.

We know that you are busy. If you would like to stay, we would be happy to have you. If you need to depart, we understand that and send you off with our thanks.

General GORDON. Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Rand Beers has filed responses to a biographical and financial questionnaire, answered pre-hearing questions submitted by the Committee, and has had his financial statements reviewed by the Office of Government Ethics. Without objection, this information will be made part of the hearing record with the exception of the financial data, which are on file and available for public inspection in the Committee's offices.

Mr. Beers, our Committee rules require that all witnesses at nomination hearings give their testimony under oath, so I would ask you to please stand at this time and raise your right hand.

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

Mr. BEERS. I do.

Chairman LIEBERMAN. Thank you, and please be seated. We would be happy to hear an opening statement at this time and would welcome also, of course, the introduction of any family or guests you have with you.

TESTIMONY OF HON. RAND BEERS¹ TO BE UNDER SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BEERS. Thank you very much, Mr. Chairman and Senator Collins. Thank you for the opportunity to appear before your Committee for confirmation. I want to thank the President of the United States for nominating me and Secretary Napolitano for recommending my nomination to the President.

I also want to take this opportunity to introduce the members of my family, without whom I surely would not be here. First, my

¹ The prepared statement of Mr. Beers appears in the Appendix on page 28.

wife, Bonnie Beers, my son, Nathaniel Beers, and my brother, Chuck Appleby, who have all come here to stand behind me. In fact, my brother has flown all the way from Vienna, Virginia. [Laughter.]

Sir, as you and others have said, I have spent about 36 years of my life working for the U.S. Government, and it is a profession that I feel honored to have been part of, and I am grateful for the opportunity with the President's nomination and hopefully with your confirmation to continue to serve the government in some capacity. The position for which I have been nominated is at the center of protecting America in the 21st Century, and I hope that my experience has prepared me amply in order to undertake this. The areas of responsibility, starting with cyber, are indeed serious and challenging.

As the President said on Friday, this is a challenge which has serious threats to the very national security of our country and requires a major response. The President has afforded the notion that the White House would have a coordinating function, but that the departments and agencies would continue to be responsible for the implementation of that policy. And as you all are aware, DHS has a major role both in the civilian side of the U.S. Government and in the private sector for drawing together the best defensive measures and the best partnership to make this Nation's cyber infrastructure secure. For that civilian side of this ledger, I am a firm supporter and believer and believe that DHS is the logical place for that responsibility to reside.

With respect to infrastructure protection, it is and represents the core of our post-September 11, 2001, protection system, with the 18 Sector Coordinating Councils, the four Cross-Sector Councils, as you mentioned, the National Infrastructure Protection Plan and the Sector Security Plans, which are now underway, the Bomb Prevention Unit, and, of course, the chemical section.

US-VISIT is at the heart of our identity management for U.S. visitors and immigrants and as such is linked not just to several of the elements within the Department of Homeland Security, but with the Departments of State, Justice, and Defense, as well. And DHS has two very important pilots in this area about which you have spoken, the Air Exit and the Land Exit programs, with which we will be working if I am confirmed.

And finally, the Risk Management and Analysis Office, which represents the brain trust for risk management tools and concepts to help the Department decision makers make the best possible decisions against the risks that we have using the resources, both monetary and personnel, to meet them.

We also have, as you mentioned, the possibility of the Federal Protective Service becoming part of NPPD, should Congress pass the required legislation for its shift. That, too, represents an important addition to the infrastructure protection responsibilities of NPPD.

I think in my briefings in NPPD that it will be an exciting place to work, with very talented people facing enormous challenges with great opportunities, and I hope that the Committee will give me the opportunity to be part of that team in confirming me as the Under Secretary.

Thank you very much, and I stand open to your questions.

Chairman LIEBERMAN. Thanks very much, Mr. Beers.

I am going to start my questioning with the standard three questions we ask of all nominees. First, 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. BEERS. No, sir.

Chairman LIEBERMAN. 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. BEERS. 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. BEERS. I do, sir.

Chairman LIEBERMAN. Thank you. We are going to start with a round of questions of 7 minutes each.

Mr. Beers, let me just get some old business out of the way before we get to the new business and just do so for the open record here. As you know, questions have been raised about something that happened when you were on the NSC staff. In 1996, you received a preliminary briefing regarding efforts by the Chinese government to influence congressional elections in the United States that year. The briefing you received later became a point of contention between the White House and the Federal Bureau of Investigation (FBI), in part because your superiors were not informed about the briefing at the time it occurred.

I wanted to ask you at the outset here if you could set that experience in context and really to ask a question in a way with the hardest edge to it. Is there any reason why your involvement in that should lead the Members of the Committee to have second thoughts about confirming your nomination?

Mr. BEERS. Senator, thank you for the opportunity to speak on the record about this. I have not to this point spoken on the record about this issue with the exception of the questionnaire, which you all asked me to fill out, and I welcome this opportunity to correct some of the characterizations and misstatements that occurred in that public discussion.

I was serving as the Senior Director for Intelligence Programs in the National Security Council staff. One of the responsibilities of the Senior Director was to be briefed on a regular basis by the Federal Bureau of Investigation with respect to counterintelligence activities that the Bureau had responsibility for. In the summer of 1996, I was briefed along with my FBI assistant by two FBI agents about a new activity that they were looking at concerning, as you mentioned, the possibility that the Chinese government was seeking in some way to influence congressional elections. The briefing itself was very preliminary, very sketchy, very limited in detail. The Bureau was unable to tell me if they had identified any individual Members of Congress or any particular congressional races that were being focused on, and the answer to that was that they were not.

As a result of that, I determined that there was not a great deal of information available but that it was something that I should continue to monitor and asked that I continue to be informed about further developments in that process.

Later on that year, there was a public controversy about Chinese efforts to influence the reelection of President Clinton and Vice President Gore, and in the course of the media discussion of that, this particular piece of information and briefing got swept up in the broader discussion, although I must say some of the media reporting suggested that this particular briefing actually referred to the presidential election rather than, as you stated, congressional elections.

Chairman LIEBERMAN. But there was no reference to the presidential election in that briefing that you received?

Mr. BEERS. None whatsoever, sir. And as a result of that, Sandy Berger, who was then the National Security Advisor, together with the White House General Counsel, launched an investigation to find out what was known, what was not known, how it had come to pass.

In the course of that particular investigation, my colleague indicated that it was his recollection that the FBI told us that we were not to brief more senior members of the White House staff. I indicated that I did not remember that particular injunction, and I indicated that had that particular injunction been communicated to me, I would have ignored it had I thought that the information was significant enough that more senior members, particularly the National Security Advisor, needed to be briefed of that.

That particular piece of information came to the media's attention and those remarks about not being permitted to brief up were attributed to me. The FBI then indicated that in no way were those briefers ever instructed to make that kind of statement, and that became part of the media swirl about all this. But I was asked not to talk to the press during that period, so I never had an opportunity to correct the record with respect to my own involvement in that.

In retrospect, looking back, I certainly think that my judgment at the time would probably have been better served had I briefed Anthony Lake, but that was my judgment, and I have to accept responsibility for that.

As a result of that, Sandy Berger gave me a verbal reprimand in the spring of 1997, and that was, as far as I know, the end of the matter, and it was not a subject of my previous confirmation hearing.

Chairman LIEBERMAN. I appreciate that very much. So as I hear it, in addition to nothing being mentioned about the presidential election, the reason you did not report up was that this was one of a number of items that the FBI was briefing you on at that meeting, is that right?

Mr. BEERS. That is correct, sir.

Chairman LIEBERMAN. And that the level of the briefing was general or vague?

Mr. BEERS. Yes, sir.

Chairman LIEBERMAN. Obviously, everybody has to make their own judgments, but certainly for myself, that is no obstacle to supporting your nomination.

I am heading to the end of my time, but let me just take us to cyber security. There was a lot of concern, certainly on this Committee and I hope more broadly, that the review and change in policy that we thought might be forthcoming from the President last week might undercut the role of the Department of Homeland Security. I was personally very relieved to see that it did not happen, at least not in what I read. Of course, for me, the reason is not just turf, it is that this is a very critical element of Homeland Security and it will continue to be so for some time to come, to protect both our non-defense Federal cyberspace and the private sector that DHS has a primary responsibility for.

Just give me your reaction. You were inside—am I reading it right? Do you feel that the role of the Directorate you would head, if confirmed, in the Department is being at least sustained, if not strengthened, and that you will not be undercut by the Cyber Security Coordinator in the White House?

Mr. BEERS. Yes, sir, that is my understanding as recently as this morning in a conversation with John Brennan that I had before I came up here for my confirmation hearing.

Chairman LIEBERMAN. Yes, on both counts?

Mr. BEERS. On both counts, that is correct. There was no realignment of roles and missions of the Department, and it is the view in the White House that the Department of Homeland Security will continue to play an absolutely essential role in the protection of America's cyber infrastructure.

Chairman LIEBERMAN. Very good. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

I want to go back to the issue in 1996 on the briefing that you received from the FBI agents who alerted you to the interest of Chinese operatives in influencing our congressional elections. I was not clear from your answer to Senator Lieberman whether you were saying that the FBI briefers told you not to report the information up the chain.

Mr. BEERS. Senator Collins, I do not remember being told that. My colleague is the person who stated that, but to the best of my memory then and to this day, I remember nothing with respect to any limitations on our ability to inform seniors—that would have been the National Security Advisor and the Deputy National Security Advisor in this case—due to the nature of the briefing.

Senator COLLINS. That leads me to ask you why you did not report the information. I know you said in response to a question from Senator Lieberman that this was one of many items and that it was not that specific, that it was vague reporting, but it seems to me that any report that a foreign country was trying to influence elections in the United States would cause you to bring that information to the attention of either the Deputy National Security Advisor or the National Security Advisor. So I am trying to better understand why you decided not to.

Mr. BEERS. Senator, if I thought that there was a program to try to influence the election that was known to be underway, I would have briefed my superiors. It was not clear to me from that briefing

that this was not more than chatter with respect to an idea. But because they were unable to brief me on any specific targets or any more detail other than the notion that there was a notion that the Chinese might be thinking about doing something like this, I felt that it was in the nature of a preliminary briefing and I wanted to have more information before I briefed more senior people.

Senator COLLINS. Did you follow up on the briefing to ask for additional briefings?

Mr. BEERS. Yes, ma'am, I did ask for additional information at that briefing. By the time this issue became a media discussion, I had not had an opportunity for a second follow-up on my own behalf. My colleague did talk to them, or at least I understand that he did talk to the Bureau about any additional information, but I was not privy to any details that there was any more information at that point in time.

Senator COLLINS. By your colleague, are you talking about the FBI detailee assigned to you?

Mr. BEERS. That is correct.

Senator COLLINS. So you did, at the conclusion of this briefing, ask your detailee to follow up and report back to you if there were subsequent developments?

Mr. BEERS. I asked both my colleague and the Bureau briefers to do the same.

Senator COLLINS. And there never was further reporting to you?

Mr. BEERS. No. In fact, I never saw any further reporting on that subject.

Senator COLLINS. So later that same year, the contributions by Chinese nationals to the presidential campaign, the Clinton-Gore campaign, became a major issue, in fact, had led this Committee to do a major investigation. At that time, did you then recall the briefing that you had had indicating that there may have been an attempt by the Chinese to influence congressional campaigns?

Mr. BEERS. I did, and I spoke to the NSC Counsel at that point in time.

Senator COLLINS. And was it at that point that Sandy Berger said to you, you should have brought this to our attention earlier?

Mr. BEERS. That is the point at which Mr. Berger and the White House General Counsel sought more information on what we knew.

Senator COLLINS. Thank you. That is very helpful.

Let me follow up with Senator Lieberman's other question, and that is on the cyber security issue. I have a lot of reservations about the establishment of a White House cyber security czar because it makes it far more difficult for Members of Congress to exercise our oversight responsibilities. We traditionally cannot call presidential advisors before the Committee. But I am also concerned in terms of accountability.

Just this past Friday, the President announced that he is creating the cyber czar, and then yesterday Secretary Napolitano appointed a number of individuals within the Department of Homeland Security with cyber security responsibilities. In your testimony, you stated that the Directorate's overarching mission is to mitigate the risk to the Nation's cyberspace by cyber criminals and nation-states.

So you have the cyber czar within the White House. You have a Director of the National Cyber Security Center within DHS. You have the head of the National Cyber Security Division. You have the Assistant Secretary for Cyber Security and Communications. And you have your position. So my question to you, Mr. Beers, is who is in charge?

Mr. BEERS. Senator Collins, thank you for that question. I think that it is an absolutely appropriate question. What Secretary Napolitano has sought to do in terms of aligning responsibilities within the Department is to create as close as possible, respecting the rules of the Senate about reorganizations of the Department of Homeland Security without recourse to congressional approval, a single chain of command that ends with the position of the Under Secretary for National Protection and Programs, which if you confirm me would be me. Working for me will be a respected cyber security individual, Philip Reitering, who is already appointed the Deputy Under Secretary for NPPD, but is now also dual-hatted as the Director of the National Cyber Security Center. Under him would be the Assistant Secretary for Cyber Security and Communications, and under him would be the office within that assistant secretaryship which carries out the specific and detailed and operational functions within the Department.

We believe that with respect to the individuals who are already in place or who are now named, we are assembling the strongest possible team that DHS could put together in order to give you and the country some assurance that DHS is here to do whatever it can, within the law, obviously, to protect America's cyber infrastructure, and I would hope that you would confirm me to be a part of that team.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins.

If I may, with Senator Akaka's permission, that was a really important question that Senator Collins asked you. I was going to ask it myself in a second round. To me, your answer was clear, which is that if you are confirmed, you will be in charge of the cyber security effort for the Department of Homeland Security.

Mr. BEERS. Yes, sir.

Chairman LIEBERMAN. Can I ask just one more quick question? On the so-called cyber czar in the White House, not yet named, do I understand correctly that the position will have no operational authority?

Mr. BEERS. That is my understanding, as well, sir. That was the discussion that went through the review study, as I was able to ascertain, and it will be a coordinating function in the tradition of the National Security Council staff, or now the National Security staff based on the new reorganization.

Chairman LIEBERMAN. Right. And what the new Cyber Security Coordinator will be coordinating is the work that you will be doing, that the NSA will be doing, that the Department of Defense will be doing. Have I left any big ones out?

Mr. BEERS. Yes, sir, you have. The Department of the Treasury, the Department of Commerce—

Chairman LIEBERMAN. Right.

Mr. BEERS [continuing]. And the Department of Justice would be three other major participants in this, as well as the rest of the civilian side of the government. As you will recall, the National Cyber Security Center and the Department of Homeland Security Cyber Security and Communications Office are together working to provide a defensive system to protect the U.S. Government from cyber intrusions. That will require our working with all of those cabinet departments and agencies, and sometimes, I am sorry to say, we need help from the White House in order to get people to play in the same sandbox.

Chairman LIEBERMAN. Understood. Thank you.

Senator Akaka, thanks for being here.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman. I am glad to be here and add my welcome to Mr. Beers and also welcome his family, wife, son, and brother to this hearing.

Mr. Beers, looking over what you have consented to do, you have a tremendous position, a tremendous job, and tremendous challenges before you. As Under Secretary for National Protection and Programs, your charge will be to take proactive steps to protect our national infrastructure and resources, and that is a huge undertaking. I am pleased with your focus on resiliency in your approach to strengthening homeland security, as well as your interest in working with partners. That is another part of your position, to work with other parts of the government at all levels, as well as the private sector. So, in looking at all of this, my feeling is that you are going to be all over the place in homeland security, but I am hopeful that you will address the human capital and management challenges within NPPD so that the Directorate can meet its operational requirements. All in all, I feel that your job is hugely operational.

In your response to the Committee's policy questions, you stated that NPPD's most significant challenge to accomplishing its mission is its ability to hire enough highly qualified employees to meet the rapidly growing demands on the Directorate. So my question to you is, what is your overall approach not only to recruiting these workers, but also to training and even retaining them?

Mr. BEERS. Senator, thank you for that question. It is truly the first challenge, if I am confirmed, that I will face, and I have thought about it. I have been briefed about it. I have talked with my colleagues about it. Philip Reitering has already begun some of the process that we need to put in place in order to bring people on board.

We have no absence of people who apply for the positions. We have no absence of people who are fully qualified for the positions. We have a problem with the process for actually taking them on board, and that represents the challenge that he has begun and that I hope I might be permitted to continue. In particular, we have to look very carefully at all of the processes leading up to the job offer and the security clearance, and that means that the processes for posting the positions, reviewing the individuals who are considered qualified, and selecting those for hiring are done in an

expeditious fashion, and they have not been always done as quickly as they might be, and Mr. Reitingger has taken that task on.

We have discussed further what more might be done with respect to the security clearance process, not to make the clearance less serious or robust, but to determine whether or not we are putting ourselves in a bind with respect to the over-classification of some of the positions, that is, positions where it might be nice to have a "top secret" clearance, but the "top secret" information would only be necessary in very rare occasions, or whether or not for those individuals who have clearances from other agencies there might be a better arrangement in order to at least grant interim clearances while the full background was done by the Department of Homeland Security, if in fact that was even necessary.

This was one of the things that the 9/11 Commission looked at in terms of the granting of clearances in the U.S. Government and the stovepipe system that currently exists, and it is certainly one that I want to examine with my colleagues if I am confirmed and one that I know the Office of the Director of National Intelligence is also interested in. So I think that there are opportunities to move from the current level of Federal employees to a higher level in a much shorter period of time than it has taken to get to the level that we are at at this particular point in time, and I regard that as a major challenge.

Senator AKAKA. Well, I am glad to hear that you look upon that as an opportunity. This is one area where we have been lacking. Senator Voinovich and I, he is the champion, have been working hard on human capital over the years, and for good reason, and we are still working on it. So your work on human capital would certainly help, and I hope, as you said, you look upon it as an opportunity.

I am pleased that you see the need to convert some contract work into career civil service positions to ensure that NPPD has the internal capacity to perform its core functions and that contractors are not performing inherently governmental work. In particular, your response to the Committee's policy questions noted that contract employees are currently serving as NPPD's Directors for Resource Administration and Human Capital. In my opinion, these seem to be inherently governmental functions. What is your timeline for converting these and other contract positions into civil service positions?

Mr. BEERS. Sir, it is my intention to move as quickly as I possibly can to make those conversions, recognizing that it is not always a one-for-one replacement. But with respect to inherently governmental functions, I want to move as quickly as possible to put in place Federal employees, recognizing that the contracting function that the Department and NPPD has may not allow the termination of the contract without financial penalties. We will have to look at all of those considerations in how we move forward, but I do not believe that it has to be a restriction in terms of bringing on board the right people for the right positions as Federal employees. So as a general answer, we will move as quickly as possible to bring people in. How quickly we can terminate the contractors and replace them will depend on the contract itself and the financial obligations of the contract.

Senator AKAKA. Well, thank you very much for your responses, Mr. Beers.

Chairman LIEBERMAN. Thank you, Senator Akaka. Senator Burris, welcome.

OPENING STATEMENT OF SENATOR BURRIS

Senator BURRIS. Thank you, Mr. Chairman and Ranking Member Collins.

I would like to welcome Mr. Beers before the Committee as we consider his nomination for Under Secretary for the Department of Homeland Security and the National Protection and Programs Directorate. Mr. Beers, from what I have read, you have a remarkable career in public service, and I was really impressed with that. I am glad to see you continuing to want to serve. Your background and demonstrated expertise in the field of national security will serve you well if you are confirmed.

I heard Senator Akaka just ask a couple of questions that I was going to ask, so let me switch back further in my notes and see if we can get you to answer this question.

You stated that although you believe the organization of the National Protection and Programs Directorate allows it to complete its mission, you would review its structure, if confirmed. Are there any specific aspects of the National Protection and Programs Directorate that you can identify at this point that will yield greater efficiencies? Would a review of the organizational structure be an immediate priority?

Mr. BEERS. Sir, I have looked at the Directorate. We have actually focused on one of the major changes that I would make, which is not so much organizational, although it would result in a different culture, and that is, move from the 50 percent level of contract employees present in our offices and move in the direction of a much higher percentage of Federal employees as quickly as possible.

With respect to organization and reorganization, the Department has put forward in the appropriation for fiscal year 2010 a major reorganization move which would move the Federal Protective Service from Immigration and Customs Enforcement to the National Protection and Programs Directorate. That would be a major reorganization, if approved. There are over 1,000 Federal law enforcement officers within the FPS, and they supervise over 15,000 contract employees which have been part of the Federal system of protecting our Federal buildings, from cabinet agencies to court-houses, around the country. That would represent a major change in both the size and management challenges. The Directorate has already begun a series of discussions and seminars with the Federal Protective Service so that if Congress approves that change, we would be ready to move as seamlessly as possible to including them within the NPPD umbrella.

Beyond that, I have some ideas that I have been tossing around in my mind, but sir, I have to say I have been around government long enough to know that, first, there is a whole lot of difference between observing an organization from the outside and observing an organization from the inside, and I am reluctant to go entirely on my preliminary visions about what I might be prepared to do.

And second, sir, I want to be able to talk to the employees specifically about this. I do not want them to hear about my thinking about reorganization without an opportunity to talk to them. So beyond the FPS proposal, there are some ideas that I have, but I would prefer not to talk about them publicly until I——

Senator BURRIS. It sounds like to me, Mr. Beers, that you are going to do the reverse. It was always contracting services. Government is contracting everything out. It looks like to me you are saying that you will look at, when those contracts expire, hiring some of those people who have been working for the contractor and bringing them back into the government. Where else are you going to get the talent and experience to bring these people in? There would be a timetable involved if you were to use individuals who are not experienced and currently working with the contractor, would that not be so?

Mr. BEERS. Sir, we have right now a hiring program for approximately 500 individuals. A number of those individuals would come on as chemical inspectors. A large other number would come to work in our National Cyber Security Division. We have had no dearth of applicants from the private sector, retired government officials, retired military and law enforcement officials, people who do come out of the contracting world——

Senator BURRIS. Well, now, if they are retired officials and they are on a pension, would they come back and have to deal with their pension arrangements with the Federal Government?

Mr. BEERS. It depends on what system they were under, sir. If they were in the military, they would be permitted to receive a second government salary in addition to their pension. If they were with a law enforcement agency, some of them would be permitted to come back and have a second contract. If they were like me, and I am a pensioner, sir, no. You get just your government salary.

Senator BURRIS. So are you telling me you are giving up your pension to come back?

Mr. BEERS. Yes, I am giving up my pension, but the amount of money I would receive if I am confirmed will be larger than my pension——

Senator BURRIS. OK.

Mr. BEERS [continuing]. Although my pension is a very generous pension for 36 years of government service.

Senator BURRIS. I would imagine so. That is a great deal of service. Thank you very much, Mr. Beers.

Mr. BEERS. Thank you, sir.

Senator BURRIS. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Burris. Senator Voinovich.

OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH. First of all, Mr. Beers, I think that we are lucky to have someone like you with experience and background who is interested in continuing to serve our country. Thank you for your willingness to do that.

Mr. BEERS. Thank you, sir.

Senator VOINOVICH. When you are confirmed, you will oversee efforts to develop and implement a biometric entry and exit system,

which Congress has been calling for since the PATRIOT Act was enacted back in 2001 and which the 9/11 Commission called an essential investment in national security. You have said that "implementing an effective air entrance and exit solution," would be one of your top priorities, if confirmed, but I notice that you excluded the word "biometric" from your description. Will implementing a biometric air entry and exit system be a priority for you?

Mr. BEERS. Yes, sir, and I regret that I neglected to use the word "biometric." It was certainly in my mind when I reviewed the answers to those questions and signed the statement. Yes, it will be biometric, sir.

Senator VOINOVICH. Recently, I met with the head of another DHS component, and he told me that he believes implementing a biometric air entry and exit system would be cost prohibitive. Do you agree with that assessment, and why or why not? Maybe you have not been around long enough to be able to answer that, but this is a pretty high up person, and he said that it would be prohibitive.

Mr. BEERS. Sir, if the solution selected involves using U.S. Government employees to implement such a system, we would have to come back to the Congress with a budget proposal that would allow us to undertake those responsibilities. We are currently looking at the pilot program. When we have the results from that pilot program and are ready to make a selection between an airline implementing solution or a government implementing solution, we will also do our homework to talk about what the cost would be, and we will come back to you with that.

Senator VOINOVICH. Now, I think—

Mr. BEERS. Whether it is cost prohibitive or not, I am not in a position at this point in time to tell you because we have not actually run the numbers in a hard fashion for that particular option.

Senator VOINOVICH. It is my understanding the airlines opted out of the biometric pilot being conducted now and that Customs and Border Protection is part of this testing and the other group that is doing it is the Transportation Security Administration (TSA).

Mr. BEERS. That is correct, sir. The airlines declined to participate in the test program. We will factor that into the pilot results and make our judgments known and work with Congress to move forward.

Senator VOINOVICH. Well, one of the things I would like to point out is that there is no money requested in the budget to actually begin implementing biometric air exit during fiscal year 2010. I understand there is more than \$20 million in prior year funds that can be used for further biometric air exit work in 2010, but the 2-month-long air exit pilot projects that US-VISIT is conducting will cost more than \$5 million. So \$20 million will not go very far. I am concerned about the lack of significant funding for this system because the Department's waiver authority to bring new countries in to the visa waiver program is linked to the creation of a biometric air exit system. Without funding, how would we move forward in fiscal year 2010 to meet congressional mandates to develop that biometric air exit system?

The point I am getting at is that we have countries now that have come into the visa waiver program, a total of eight new ones. There are no other countries ready to come in right now, but there may be, I think, in 2010. But the statute provides that if the biometric air exit system is not in place, then the Secretary authority to waive visa refusal rates exceeding 3 percent stops. That is, you cannot bring in many more countries, so aspirant countries go into limbo. And my concern is that if we do go forward with biometric air exit, and you said you think it is a good idea, then I think there ought to be some money so that you can implement it and we do not end up, as I say, in limbo with our visa waiver program expansion, which is not only important to our national security, but also to public diplomacy for this country because there are a lot of countries out there right now that would like to get into the program and are hoping to get in, but without this system, they cannot be waived in.

Mr. BEERS. Sir, you are absolutely right in that regard. It would appear to me, as well, that \$20 million would not be enough to implement that kind of a program if it becomes a government program, and that is why I said what we need to do at the conclusion of the pilot test is come forward with, first of all, where we think the solution ought to go and, if it is a government program, with a way to pay for it because I am committed to it and want to work with you and other Members of Congress to implement that program because I believe it is important to the security of this country.

Senator VOINOVICH. Well, I may call the Secretary because I am Ranking Member on that Homeland Security Appropriations Subcommittee and maybe we could stick some money in there so that if you do decide to go forward with it, you have some money to work with and we can move forward with it.

In 2007, DHS released scorecards evaluating the interoperable communications capabilities with major cities. I took it upon myself to visit the four cities in Ohio where those scorecards were issued. I thought the scorecards were terrific because they showed that we only had one city that really was up to snuff in Ohio. The rest of them were not there. I would like to suggest to you that those scorecards were a great idea, and I would hope that you might revisit that program so that we could go out and do another evaluation of where cities are to see if they have made any improvements because interoperability is fundamental, I think, to any kind of response to either a natural disaster or a terrorist attack.

Mr. BEERS. Sir, you and other Members of this Committee and the Congress have made that clear to us, and I totally agree with you that this is an absolutely vital program to protecting America, and I look forward to working together with you and other Members of this Committee to make that program a reality. So you have my commitment to that.

Senator VOINOVICH. Thank you.

Chairman LIEBERMAN. Thank you. Well done.

Let us do a second round of 5 minutes each, if Members have additional questions.

Mr. Beers, let me focus on the Office of Infrastructure Protection that comes under the Directorate you have been nominated to

head, which is now, as you said, tasked with coordinating a national program to reduce the risk to the Nation's 18 critical infrastructure and key resources sectors. These sectors are wide-ranging and include areas such as energy, information technology, water, and financial—really the basis of the way we live in our country today. All of them are critical, but obviously we have limited resources and therefore prioritization is necessary.

I would say up until this point that the transportation and chemical sectors have been a focus of the Department. Are there sectors that you believe have not yet received adequate focus and should now become added to the Department's top priority list?

Mr. BEERS. Sir, one of the major reasons that I took this job was the cyber function that was embedded in this job—

Chairman LIEBERMAN. Yes.

Mr. BEERS [continuing]. And in that particular sector and the cross-sector committee on cyber security, that would be one of my major efforts in the 18 critical sectors. The second would be the electrical sector. It is hard for cyber security to work without electricity. It is hard for the critical infrastructure, cyber infrastructure, to work without electricity. So I would want to make sure that we were as confident as we might be that those two sectors were receiving as much attention as needed.

I do not want to in any way, however, diminish the importance of the other sectors—

Chairman LIEBERMAN. Sure.

Mr. BEERS [continuing]. But you asked for the principal ones that I would focus on at the start, and those are the two, sir.

Chairman LIEBERMAN. Well, that is a helpful and encouraging answer. One related question is we know, of course, that today, electricity depends on cyber systems, as well. In 2007, the Department of Homeland Security, working with the Idaho National Laboratory, discovered a cyber vulnerability known as "Aurora," which has the potential to do really long-term costly damage to mechanical equipment essential to the operations of the electric sector. The reality is that if vulnerabilities like Aurora are strategically compromised in a coordinated manner, large portions of the United States could be without electricity for a long period of time.

Do you believe that current efforts to secure the electric sector from cyber attack are sufficient? If not, give us a general idea what your plan would be to try to improve them.

Mr. BEERS. Sir, you are absolutely right in referring to that study in terms of the significant vulnerability. I do not believe we have adequately addressed that vulnerability or other vulnerabilities, and that is why I intend to look at the individual protections for these data systems that serve as the controls for the electrical grid and specifically at those generators that were deemed to be so vulnerable. I think we need to erect our cyber defenses not just in the U.S. Government, but ensure that the private sector is aware of the possibilities and takes advantage of those defenses insofar as they can bring them to bear on the vast amount of our critical infrastructure that is in the private sector.

Chairman LIEBERMAN. Well, I appreciate that answer. I appreciate what you said earlier, that cyber defense is probably the No. 1 reason why you have taken on this assignment. Part of the chal-

lenge obviously is how do you and all those working with you in the Department of Homeland Security get the private sector, which owns and operates most of the critical infrastructure, to do what needs to be done to protect our homeland security, particularly if it costs money to do it at a difficult economic time.

I will come back to this with you, Mr. Beers, but I hope as you go through these issues, if you are confirmed, at the beginning of your service in this position, if you feel that you need additional legislative authority to get the private sector to do what we need them to do in the national interest, I hope you will not hesitate to let this Committee know.

Mr. BEERS. Thank you, sir. I will.

Chairman LIEBERMAN. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

I want to follow up on an exchange you had with Senator Voinovich, who talked about the importance of interoperable communications. This has been a priority of the Chairman and mine for several years, and we made some progress, but not enough.

Several years ago, the Integrated Wireless Network project was begun and the goal was to create a nationwide consolidated interoperable wireless communications system for the law enforcement officials at the Department of Homeland Security, the Department of Justice, and the Treasury Department. Despite spending hundreds of millions of dollars, a Government Accountability Office (GAO) report in December of last year found that the program had failed, and it had failed due to a lack of leadership within the participating agencies. In the Department of Homeland Security's response to the GAO report, the reason given for abandoning the joint program was "because the Department of Justice and DHS have different regional priorities, a common system will not work at the national level." Now, keep in mind this is after spending hundreds of millions of dollars to achieve this.

What is your view of having an interoperable communications system for Federal law enforcement officers regardless of which agency they are employed by?

Mr. BEERS. First of all, as a general proposition, Senator Collins, I am committed to that objective. I think that it just makes really good common sense. I understand that the Department has spent a large amount of money without success, although I am told that there was a successful test bid in the Pacific Northwest that seemed to be operating effectively. But you are right about the GAO report conclusion and the statement that the Department gave you in response to that GAO report.

I am committed to looking into this. I understand that the concept of the Emergency Communications Preparedness Center is a hoped-for solution to this problem, but it is the kind of thing that I am going to have to dig into if I am confirmed and probably work further with you all in order to get the right answer. But I am committed to getting to yes in this general proposition. The notion that somehow we cannot find a common solution just because different departments and agencies have different ways of doing business is kind of the same thing that we are wrestling with US-VISIT, which is how do you merge the databases that different departments and agencies have in order to have the most effective common database.

And I am not saying that it is easy, but it also seems to me that it is something that a little bit of elbow grease and attention might be able to resolve a little more easily than throwing up your hands.

Senator COLLINS. I certainly agree with you. The Department's response to the GAO report sounds like a turf battle to me rather than focusing on what the objectives should be. It is certainly ironic that the Department—correctly, in my view—has pushed State, regional, and local law enforcement to work together on interoperable systems and yet has thrown up its hands and apparently abandoned an attempt to have an interoperable system across the Federal Government. So I am pleased to hear your response, and we look forward to working with you on that.

Let me switch to another issue, which is the chemical security law, which as an author of that law is of great interest to me. I read with interest that in 2006, you co-chaired a task force on homeland security established by the Century Foundation, which issued a report that had a chapter on chemical site security. Now, this was before we were successful in getting the law passed. But you have two recommendations that are not included in the current law. One was to provide liability protection and the other terrorism insurance premium reductions for chemical plants that are in compliance with the Federal chemical security regime. Do you still agree with those recommendations, or is it something you would still pursue?

Mr. BEERS. It is something that I certainly want to look at in the context of the chemical legislation reauthorization, although, as you know, the Administration only asked to roll over the existing authorization in this fiscal year in order to give ourselves in the Executive Branch time to make sure that we had the right answer to that question.

I would certainly like to look at that, if I am confirmed, as an element. As I said earlier, being on the inside and looking in from the outside are two different perspectives. I am not saying that my perspective will not change. I am not saying that it will change. But I certainly want to take the opportunity to look at this reauthorization and thank all of you on this Committee for that legislation. I care deeply about that, as indicated in that book and efforts that I undertook to look at this issue from the time that I left government, and so you all are to be commended for a terrific piece of legislation.

Senator COLLINS. Thank you. I appreciate that. This Committee has tried to identify gaps and emerging vulnerabilities and pass legislation to try to get ahead of the curve, and I will be looking forward to your recommendations. I am aware that the Department and the Administration has asked for a one-year extension of the sunset deadline, or the expiration of that law, and we look forward to working with you.

Just one final question. In your responses to Senator Lieberman and in your responses to the pre-hearing questions, you indicated your willingness to respond to requests for information from this Committee. I would be remiss in my duties as the Ranking Minority Member if I did not ask that you treat requests from the Chairman and from the Ranking Member equally, even though I can assure you that 90 percent of the time, those will be joint requests

and this Committee prides itself on its bipartisan approach to these issues. But would you respond to requests from the minority equally?

Mr. BEERS. Without reservation.

Senator COLLINS. Thank you.

Mr. BEERS. I have worked for Administrations in which the Executive Branch and the Legislative Branch were not always led by the same party, and I have worked when they were the same party, and I have worked with both parties and served both parties. I look forward to working with the minority as well as the majority.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins.

I want to give you a special assignment, Mr. Beers, in your review of the Chemical Facility Anti-Terrorism Standards Act. It is called CFATS, which has become pronounced in government circles as "see-fats." We can do better than that, and I am counting on you. [Laughter.]

Mr. BEERS. Thank you, sir. That is a challenge.

Chairman LIEBERMAN. I think they have a whole unit over at the Pentagon because in the Pentagon, this would be called Operation Sturdy Strong Cleanup or something. [Laughter.]

Senator BURRIS.

Senator BURRIS. Thank you, Mr. Chairman. I just have a general question.

Mr. Beers, Homeland Security is a relatively new Department. It was a conglomeration of responsibilities coming from various other sources and agencies. If you are confirmed, do you think that you will have a pretty good working knowledge to pull all of those functions together and overcome all the turf battles? Do you see any turf battles that might be inhibiting you at this point to carry out NPPD's major functions?

Mr. BEERS. Sir, you are absolutely correct in your characterization of the Department, and the evolution of this bringing together of a number of different agencies from different departments was a challenge at the beginning and continues to be an ongoing issue. It is certainly one that Secretary Napolitano recognized when she took over the Department and one which she has listed as one of her five major priorities.

There are some rivalries. There are some turf battles. I do not believe that any of them are insurmountable, but I also have to tell you in all candor, sir, I served much of my career in the Department of State, and to say that there are not turf battles in the Department of State among the offices in that Department would be to ignore over 100 years of history in that particular Department. So it is not always true that the passage of time resolves all challenges, but it is certainly one that the Secretary and I, if I am confirmed, will take on as an important issue, to make sure that she says we have one DHS and not 37 different entities within a Department.

Senator BURRIS. Yes, because I see that you are going to take over, what is it, the FPC, or—

Mr. BEERS. FPS, sir. The Federal Protective Service.

Senator BURRIS. Yes. So if you begin to try to move that away, I can just see that there might be some turf problems starting there if that were the case.

Mr. BEERS. Sir, that is an interesting question because there has been a lot of discussion about where the Federal Protective Service would be best located, including some people who have said that perhaps it ought to go back to the General Services Administration from which it was plucked and put into the Department of Homeland Security.

Senator BURRIS. I used to run a similar General Services for the State of Illinois—

Mr. BEERS. Yes, sir.

Senator BURRIS [continuing]. And have had this experience of turf problems.

Mr. BEERS. Yes, sir. When you think conceptually about what that law enforcement agency does, protecting Federal critical infrastructure, and the responsibility of the Infrastructure Protection Office in NPPD, there really is, I think, an alignment here of missions, and one of our sectors is the Federal, State, local, tribal, and territorial governmental infrastructure. So this actually, I think, represents a good conceptual fit. Now, if that happens, what NPPD will need to do is make sure that the transfer from Immigration and Customs Enforcement to NPPD is done as smoothly as possible so that the normal turbulence associated with any kind of a move of that magnitude does not come to be crippling to the roles and missions of the FPS or NPPD.

Senator BURRIS. Mr. Beers, I want to congratulate you and look forward to you continuing your work with public service. I am just admiring your ability to come back and extend that talent and commitment that we need at such a crucial time. Congratulations to you.

Mr. BEERS. Thank you, sir, for your kind words.

Chairman LIEBERMAN. Well said, Senator Burris.

Thanks, Mr. Beers, for your testimony today, for your willingness to serve. If confirmed, you are going to be in a truly critical position for our homeland security, and your entire career, fortunately for us, prepares you for it, so I thank you for your willingness to serve again. I thank your family for backing you up. We have almost a reflex reaction that is quite appropriate in the Armed Services Committee of thanking the nominees and their families. We probably do not do that enough in the other committees, so we thank the people behind you.

Without objection, the record for this hearing will be kept open until 12 noon tomorrow for the submission of any written questions or statements for the record, and we hope very much to be able to move your nomination out of the Committee and through the Senate as soon as possible.

Do you have anything else you would like to say in your defense before we execute judgment? [Laughter.]

Mr. BEERS. No, sir. Thank you very much for the opportunity to appear before you and to answer your questions. It was a pleasure.

Chairman LIEBERMAN. Thank you. Senator Collins.

Senator COLLINS. Mr. Chairman, I just want the nominee to know that I have introduced a bill to allow the reemployment of

annuitants without having their pensions offset in order to help us attract people back into government. However, in your case, the bill, I regret to tell you, would not apply because it is limited to part-time work over a limited period of time, and if all goes well, we hope that you will not be doing part-time work when you are at the Department.

Thank you, Mr. Chairman.

Mr. BEERS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins.

The hearing is adjourned.

[Whereupon, at 3:55 p.m., the Committee was adjourned.]

A P P E N D I X

Prepared Statement of Joseph Lieberman

The Nomination of Rand Beers to be Under Secretary for the National Protection and Programs Directorate June 2, 2009

Good afternoon. Thank you all for coming to our hearing today on the nomination of Rand Beers to be Under Secretary for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security (DHS).

Mr. Beers is a highly-qualified nominee with a record of more than 30 years of public service, dating back to his service as a Marine in Vietnam. He has served in Democratic and Republican administrations, working as the Senior Director for Combating Terrorism at the National Security Council (NSC) during the Administration of George W. Bush, as Assistant Secretary of State for International Narcotics and Law Enforcement Affairs during the Clinton Administration, and Director of Counter Terrorism and Counternarcotics at the NSC for the Administration of George Herbert Walker Bush. More recently, Mr. Beers played a key role in the transition at the Department of Homeland Security from the Bush to Obama Administrations and has been a chief counselor to Secretary Napolitano since that time.

If confirmed, Mr. Beers will be required to apply his wealth of experiences to harness and provide vision for the National Protection and Programs Directorate, which includes programs covering cyber security, infrastructure protection, foreign traveler screening, and emergency communications. The President's FY2010 budget proposes to expand this Directorate further by moving the Federal Protective Service into the NPPD.

Cybersecurity is clearly one of the directorate's top priorities. The threat of cyber attacks is an urgent national security challenge. Last week, President Obama announced the results of the 60-day review of cyber security policy and government structures, and I am grateful for the President's focus on this issue. We believe, and the President has confirmed, that DHS has a central role to play in any government-wide cyber security strategy, and NPPD will lead the Department's efforts in that regard. I look forward to hearing what Mr. Beers thinks the Department's role should be and how he will ensure that DHS has the necessary tools to perform its job.

NPPD's critical infrastructure responsibilities are no less challenging. Because the majority of the nation's critical infrastructure – our energy, communications, and transportation networks, for example – are owned and operated by the private sector, DHS must work closely with the private sector to put appropriate security structures in place.

The lesson from the Mumbai, London, and Madrid attacks is that terrorists will seek out "soft targets" such as hotels, shopping districts, and inner city transit lines. So we must accelerate our efforts to harden those targets.

NPPD also plays a critical role in our nation's security through the US-VISIT program, which requires foreign nationals to undergo biometric screening as they enter the country. The 9/11 Commission concluded that three of the September 11 hijackers had overstayed their U.S. visas, and concluded that requiring biometric exit screening was vital to homeland security. In fact, if we had implemented a biometric system to detect overstays prior to 9/11, we could have prevented the attacks of 9/11. I am very concerned that almost eight years later, despite the clear need for a viable biometric exit system to ensure that we know when foreign nationals overstay their visas, we still do not have a workable exit system in place. This committee will continue to work with DHS to ensure that a secure biometric exit system is expeditiously deployed at the nation's airports.

Many other challenges face the NPPD, including the future of chemical security, the directorate's challenge in hiring and retaining qualified staff, and the over dependence on contractors to do what otherwise might be considered inherently governmental work. I intend to work closely with the new Under Secretary to reauthorize and strengthen the Department's Chemical Facility Anti-Terrorism Standards (CFATS), the chemical security site program.

I also want to discuss with him whether DHS is becoming so dependent on contractors that it risks having too little in-house ability to evaluate the solutions its contractors propose, or to develop options on its own. And I want to know how he intends to attract and hire the necessary permanent staff to fulfill the directorate's critical missions.

Mr. Beers is an experienced public servant of long standing. If confirmed, his expertise will be put to good use at NPPD. I look forward to hearing his views on the direction of the Directorate.

Prepared Statement of Senator Susan M. Collins

**Nomination of Rand Beers to be Under Secretary of the National Protection
and Programs Directorate at the Department of Homeland Security**

Committee on Homeland Security and Governmental Affairs

June 2, 2009

I join the Chairman in welcoming Rand Beers as the nominee to be Under Secretary of the National Protection and Programs Directorate, or NPPD, at the Department of Homeland Security.

As the Chairman has indicated, the scope and importance of the NPPD's responsibilities are daunting. NPPD is charged with:

- ensuring successful implementation of the chemical-facility security program that was authorized in 2006 due to the work of this Committee - a program that will need to be re-authorized this year;
- assessing risks to our nation's critical infrastructure;
- leading DHS's effort to protect our nation against Improvised Explosive Devices and working to combat terrorists' use of explosives in the United States; and
- protecting the nation's cyber networks.

This last responsibility - cybersecurity - is both critical and complex. The complexity arises not just from the technical nature of the issue, but from the disjointed approach the federal government has taken. In the course of the coming months, cybersecurity responsibilities across the federal government will be debated as we consider the Administration's plan and alternative legislative proposals.

DHS's relationships with the critical infrastructure sectors that both provide for and rely on information technology services will remain invaluable in ensuring a coordinated defense against cyber attacks. I look forward to hearing from Mr. Beers about how, if confirmed, his management of DHS cybersecurity efforts will be affected by the White House's new cybersecurity initiative.

NPPD also manages programs that benefit components across the Department, including the US- VISIT program that screens the biometrics collected from visitors to the United States against immigration and criminal databases. US-VISIT has been struggling for years with implementing a solution to collect biometric information on foreign travelers departing the country - a responsibility that is required by law.

Should Mr. Beers be confirmed, these are just some of the critical challenges awaiting his leadership and expertise.

Hearing on the Nomination of:

**Rand Beers
To be Under Secretary of the
United States Department of Homeland Security**

**Before the
United States Senate Committee
on Homeland Security and Governmental Affairs**

**June 2, 2009
342 Dirksen Senate Office Building**

Mr. Chairman, Senator Collins, and Members of the Committee, I am honored to appear before you today. I am humbled by the confidence that President Obama and Secretary Napolitano have placed in me by nominating me for the position of Under Secretary of the Department of Homeland Security. If confirmed, I hope to work closely with you to address the critical challenges facing the National Protections and Programs Directorate (NPPD).

At this point, I want to recognize my wife Bonnie Beers without whom I would not be here today and my two children, Drs. Nathaniel and Benjamin Beers.

In your respective opening statements for Secretary Napolitano's confirmation hearing in January, you recognized the progress that DHS has made to date, and outlined priorities for the work that must now be addressed by both the Department and this Committee. Notably, many of these key issues fall under NPPD's responsibilities.

For example, you both highlighted the need to reauthorize the expiring chemical security legislation. Chairman Lieberman raised the issues of furthering border security progress, and bringing rail and transit security on par with improvements to air travel – areas that NPPD supports through the US-VISIT program, cross-sector critical infrastructure protection, and through partnerships with Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), the Coast Guard, and the Transportation Security Administration (TSA). Senator Collins, you emphasized the importance of an empowered cybersecurity expert who can “enforce best practices across the federal government” and improve coordination with private sector cyber stakeholders. You also called for increased critical infrastructure protection, including improved cooperation with the private sector and efforts to “strengthen the framework embodied in the National Infrastructure Protection Plan.”

I fully share your focus on these essential issues, and if confirmed, will work diligently with you to address these and all NPPD's duties. NPPD needs an appropriately sized federal workforce to accomplish its missions, and I am dedicated to recruiting the right talent while reducing the time needed to bring those we've selected on board. If confirmed, my priorities would be to:

- Continue building NPPD's capabilities to defend the nation's cyberspace.
- Continue to increase the security of the country's chemical facilities by building a strong Chemical Facilities Anti-Terrorism Standards (CFATS) program.
- Strengthen our private sector partnerships to allow for increased information sharing and coordination among the federal, state, local, tribal, and territorial governments and private industry regarding the protection of critical infrastructure and key resources.
- Secure our nation's borders by implementing an effective Air Entrance and Exit solution.

I have served this nation in the field and here in Washington since 1964, from the fields of Vietnam, to the embassies and headquarters of the Department of State, as well as on the National Security Council (NSC) and the White House staffs. My engagement in

critical infrastructure far predates the establishment of DHS, serving in the mid-1990s as the NSC Staff lead for the Presidential (Marsh) Commission on Critical Infrastructure Protection, and beginning the follow-on work on the first Presidential Decision Directive (PDD) on the subject – PDD 63.

In the decades that I have worked on the prevention of and response to terrorism, I have been involved in some of the most prominent cyber and critical infrastructure challenges this country has faced. I have rare first-hand knowledge of how inherently interdependent traditional critical infrastructure protection and cybersecurity are. For example, my NSC colleagues and I were involved in the immediate response to the first World Trade Center bombing in 1993 when the New York Fire Department was encouraged to allow members of a bond trading company to return to the evacuated top floors of that building to recover data so that open trading positions in billions of dollars left hanging in cyberspace could be closed out in order to restore stability in the financial markets. Subsequently, we worked with the financial sector to bolster redundancies and resiliencies within the system.

Existing gaps in cybersecurity pose a tremendous vulnerability to our nation, and, if confirmed, I intend to support Secretary Napolitano in bringing the right people, strategy, and resources to bear in this area. The Directorate's Office of Cybersecurity and Communications has made significant strides in advancing the Department's cybersecurity efforts, however much more needs to be done. This process has begun already, as the Secretary recruited Phil Reiting to serve as the Deputy Under Secretary at NPPD, and to take the lead for DHS on cyber issues. Phil brings unquestioned public and private-sector expertise into the cyber arena, and he embodies the quality of personnel I hope to bring to NPPD in addressing the need for a strong government workforce across the directorate. I believe that my experience in the interagency process and in cyber issues will complement Phil's expertise and ensure that DHS's cyber equities are fully represented and remain at the forefront of the national effort.

As I have stated, another priority for the Department, the Directorate, and this Committee is the continued implementation of the Chemical Facility Anti-Terrorism Standards (CFATS) program. I firmly believe CFATS is an effective program for addressing the security risks associated with the nation's high-risk chemical facilities, and is a key program in making our nation more secure. Since the Department was granted authority to regulate security at high-risk chemical facilities two and one-half years ago, I believe the Department has developed an effective approach for both identifying high-risk chemical facilities and assessing the security risks associated with them. If confirmed, I look forward to working with the Committee and Congress to reauthorize the program.

As this Committee knows well, the Department of Homeland Security also has a unique federal role in bridging our nation's security interests with the concerns and needs of the private sector. Particularly in physical critical infrastructure protection and cybersecurity where the overwhelming majority of assets are not government-owned, partnership with the private sector is paramount to our nation's success. NPPD must be the government's lead in fostering such cooperation for the common good. If confirmed, I will seek private

sector input at the outset of the policymaking process to ensure that they are true stakeholders in developing comprehensive national solutions to the joint issues we must address.

The Directorate's Office of Infrastructure Protection (IP) has worked diligently with our partners over the past several years in standing up the National Infrastructure Protection Plan (NIPP) framework, which in my opinion has greatly benefited the collaboration between the Department and our federal and private sector partners. If confirmed, I look forward to working closely with IP to ensure that we continue our emphasis on the NIPP partnerships and, in fact, strengthen these efforts with state, territorial, tribal and local jurisdictions, regional coalitions, and State and local fusion centers.

Furthermore, the President's Fiscal Year 2010 budget would transfer the Federal Protective Service (FPS) from the U.S. Immigration and Customs Enforcement (ICE) to NPPD. FPS has distinguished itself for its expertise in physical security operations and its mission complements those of the Directorate's other core missions. If approved by Congress, I believe this move aligns the federal critical infrastructure protection mission of FPS with those under the direction of the Directorate's Office of Infrastructure Protection and enhances the Department's ability to fill its crucial role in leading our nation's efforts to protect critical infrastructure and key resources.

If confirmed, I intend to further strengthen and develop NPPD's US-VISIT program, a critical component of the Directorate and the Department's mission of securing our national borders while facilitating legitimate travel and trade. As the Committee knows, US-VISIT works collaboratively across the Department - with ICE, CBP, the Coast Guard, and TSA - as well as with the federal interagency process - including the State Department, the Justice Department and Defense Department - on a number of efforts to enhance security, increase efficiency of screening processes, and improve identity management. Through US-VISIT, these DHS partners have prevented thousands of ineligible and potentially dangerous persons from entering our country as well as those apprehended while illegally crossing the border or present in the interior of our country. And through the Secure Communities effort operated by ICE, local law enforcement officers have identified criminal aliens who were incarcerated in state and local jails by accessing the biometric information managed by US-VISIT. I am particularly interested in the development and outcome of the air exit pilot program, and I fully recognize the implications that air exit holds for related efforts such as the Visa Waiver Program (VWP), and large-scale issues such as national security and immigration. If confirmed, I look forward to working with Members of this Committee and Congress at large as we move forward on this critical component of the US-VISIT program.

I see the Directorate's overarching mission to be the mitigation of risk to the nation and its citizens: the risk to the nation's critical infrastructure by manmade or natural disasters; the risk to the country's cyberspace by cyber criminals and nation-states; and the risk of individuals entering into this country with the intent to do harm. To this end, the Directorate, through the Office of Risk Management and Analysis (RMA), has a leadership role in synchronizing, integrating, and coordinating risk management and risk

analysis approaches within DHS. RMA has made progress, but I believe more needs to be done. Of note, RMA has worked to develop the DHS Risk Lexicon through the Department's Risk Steering Committee and completed the prototype for the Risk Assessment Process for Informed Decision-making (RAPID), to inform strategic policy and budgetary decision-making by taking into account risk, risk reduction efforts, and alternative resource allocation strategies. If confirmed, I plan to continue to support RMA in its efforts to work collaboratively across DHS and with our homeland security partners to build an integrated risk management program that ensures that risk information and analysis are provided to decision-makers to inform their decision-making in the allocation of time, people, and funding.

Mr. Chairman and Members of the Committee, we stand at a juncture in homeland security where the challenges and the opportunities are enormous and the missions of NPPD are at the forefront. I ask that you afford me the opportunity to take up the leadership mantle and help build and direct an empowered NPPD workforce to address these challenges.

BIOGRAPHICAL AND FINANCIAL INFORMATION REQUESTED OF NOMINEES

A. BIOGRAPHICAL INFORMATION

1. **Name:** (Include any former names used.)
 - Rand Brittingham Beers. I have also used the following names: Robert Rand Beers, R. Rand Beers, Robert Rand Appleby (mother's remarried name, used from age 4 to 15), nickname Randy
2. **Position to which nominated:**
 - Under Secretary, Department of Homeland Security
3. **Date of nomination:**
 - April 20, 2009
4. **Address:** (List current place of residence and office addresses.)
 - Home: REDACTED
 - Office: Department of Homeland Security, Nebraska Avenue Complex, Washington, D.C. 20548
5. **Date and place of birth:**
 - 11/30/1942
 - Washington, D.C.
6. **Marital status:** (Include maiden name of wife or husband's name.)
 - Married to Marion Alice Brittingham Beers (Maiden name – Brittingham)
7. **Names and ages of children:**
 - Nathaniel Brittingham Beers, age 38
 - Benjamin Brittingham Beers, age 34
8. **Education:** List secondary and higher education institutions, dates attended, degree received and date degree granted.
 - Episcopal High School, Alexandria, Virginia, 1958-60, HS Diploma, June 1960
 - Dartmouth College, Hanover N.H., 1960-64, BA, June 1964
 - University of Michigan, Ann Arbor, MI., 1968-71, MA, June 1970 (Note: I was in a PhD program during this time, and also spent time from 1978-1979 working on my PhD but did not finish my dissertation. The subject was military history.)
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.)
 - April 3, 2009 – present and January 21– February 11, 2009
 - Counselor to the Secretary, Department of Homeland Security

- February 11 – April 3, 2009
 - Acting Deputy Secretary, Department of Homeland Security
- September 2008 – January 2009
 - Worked on the Obama transition effort, Department of Homeland Security, Volunteer
- 2005 – 2009
 - President, National Security Network (previously called Alliance for American Leadership and Valley Forge Initiative)
- 2006 – 2007
 - Good Harbor Consulting, Contract Consultant
- July 2004 - 2008
 - Adjunct Professor, Kennedy School of Government, Harvard University
- 2004
 - Adjunct Professor, Georgetown University
- 2003 - 04
 - National Security Advisor, John Kerry Campaign for President
- 2002-2003
 - Senior Director for Combating Terrorism, National Security Council
- 1998-2002
 - Assistant Secretary for International Narcotics and Law Enforcement Affairs, United States Department of State
- 1995-98
 - Senior Director for Intelligence Programs, National Security Council
- 1993 - 1995
 - Director for Peacekeeping, National Security Council
- 1992-93
 - Deputy Assistant Secretary for Regional Affairs, Bureau of Politico-Military Affairs, United States Department of State
- 1988-92
 - Director for Counterterrorism and Counternarcotics, National Security Council
- 1971-88
 - United States Department of State
 - 1986-88, Deputy for Strategy, Bureau of Politico-Military Affairs
 - 1984-86, Office Director, Office of Regional Affairs, Bureau of Politico-Military Affairs
 - 1979-84: Politico-Military Officer, Bureau of Politico-Military Affairs; Deputy Office Director, Office of Policy Analysis, Washington, D.C.
 - 1978-79: Leave without pay working on PhD, Washington, D.C.
 - 1976-78: Population Affairs Officer, Bureau of Oceans, Environment and Science, Washington, D.C.
 - 1975-76: Attended Foreign Service Institute Economics Course, Arlington, Va.

- 1973-75: Deputy Political Advisor to Supreme Allied Commander Europe (SACEUR), Supreme Headquarters Allied Powers Europe (SHAPE), Casteau, Belgium
 - 1972-73: Politico-Military Officer, Bureau of Politico-Military Affairs, Washington, D.C.
 - 1971-72: Attended A-100 Orientation Course, Arlington, Va.
 - 1964-68
 - United States Marine Corps
 - 2nd Lieutenant to Captain;
 - Basic School, Basic Officer Training, Quantico, VA.
 - Platoon Commander, 2d Battalion, 2d Marines, Camp Lejeune, N.C.
 - Platoon Commander, 1st Military Police Battalion, Camp Pendleton, CA
 - Platoon Commander, 1st Military Police Battalion, Vietnam
 - Regimental Deputy Operations Officer, 2d Marines, Vietnam
 - Company Commander, I Company, 3rd Battalion, 3rd Marines, Vietnam
 - Guard Officer, Marine Security Guard Unit, Norfolk Naval Base, Norfolk, 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.
- National Security Network, President, 2005-2009
 - National Security Initiative, President, 2005-2009
 - Markle Foundation
 - Good Harbor Consulting, LLC
12. **Memberships:** List all memberships, affiliations, or and offices currently or formerly held in professional, business, fraternal, scholarly, civic, public, charitable or other organizations.
- Zeta Psi Fraternity, Dartmouth College, 1961-64;
 - President Stoddert Soccer League, 1982-85
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.
- Served as an advisor and foreign policy expert resource to Democratic Congressional and Senate Candidates in the 2006 and 2008 election cycle
 - Worked on the Obama campaign as a volunteer (2007-2008)
 - National Security Advisor, John Kerry Campaign for President (2003-2004)
- (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.
- Congressman Joe Sestak 2006: \$1000
 - Congressman Joe Sestak 2007: \$250
 - Obama for President 2008: \$2300, spouse \$2300
14. **Honors and awards:** List all scholarships, fellowships, honorary degrees, honorary society memberships, military medals and any other special recognition for outstanding service or achievements.
- None
15. **Published writings:** Provide the Committee with two copies of any books, articles, reports, or other published materials which you have written.
- The Forgotten Homeland, A Century Foundation Task Force Report, chaired with Richard Clarke, 2006
 - Untitled article on torture, Washington Monthly, Jan/Feb/March 2008
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.
- Speech delivered to the American Academy of Diplomacy in Philadelphia and Chicago in fall 2007 and spring 2008.
 - Testimony before the U.S. Congress Joint Economic Committee, "*Iraq: The Cost to America's Security*," February 28, 2008.
- (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.

- Testimony before the Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security, "*Narco-Terror: The Worldwide Connection Between Drugs and Terrorism*," March 13, 2002.
- Testimony before the Senate Committee on Appropriations, "*Foreign Operations, Export Financing, and Related Programs Appropriations for Fiscal Year 2002*," May 8, 2001.
- Testimony before House Committee on Government Reform, "*Study of Plan Colombia: An Assessment of Successes and Challenges*," March 2, 2001.
- Testimony before Senate Committee on Foreign Relations, "*Review of the Anti-Drug Certification Process*," March 1, 2001.
- Testimony before Senate Caucus on International Narcotics Control, "*Plan Colombia: An Initial Assessment*," February 28, 2001.
- Testimony before House Committee on Government Reform, "*Getting U.S. Aid to Colombia*," October 12, 2000.
- Testimony before House Committee on International Relations, "*Implementing Plan Colombia: The U.S. Role*," September 21, 2000.
- Testimony before Senate Caucus on International Narcotics Control, "*Ecstasy: Underestimating the Threat*," July 25, 2000.
- Testimony before House Committee on Government Reform, "*Counterdrug Implications of the U.S. Leaving Panama*," June 9, 2000.
- Testimony before Criminal Justice, Drug Policy and Human Resources Subcommittee, House Committee on Government Reform, "*Counternarcotics Cooperation with Panama*," June 9, 2000.
- Testimony before Senate Committee on Armed Services, "*U.S. Support for Counter-Narcotics Activities in the Andean Ridge and Neighboring Countries and the Impact of Narcotrafficking on the Stability of the Region*," April 4, 2000.
- Testimony before the House Armed Services Committee, "*2001 National Defense Authorization Act: U.S. Policy Towards Colombia*," March 23, 2000.
- Testimony before Senate Caucus on International Narcotics Control, "*Review of President's Annual Certification Process*," March 21, 2000.
- Testimony before House Committee on Appropriations, "*Foreign Operations, Export Financing, and Related Programs Appropriations for 2001, Part 2*," February 29, 2000.
- Testimony before House Committee on Armed Services, "*Hearings on National Defense Authorization Act for Fiscal Year 2001*," February 8, 2000.
- Testimony before Senate Committee on Foreign Relations, "*2000 Foreign Policy Overview and the President's Fiscal Year 2001 Foreign Affairs Budget Request*," February 8, 2000.
- Testimony before House Committee on Government Reform, "*Cuba's Link to Drug Trafficking*," November 17, 1999.

- Testimony before Senate Caucus on International Narcotics Control, "*Colombia: Counter-Insurgency vs. Counter-Narcotics*," September 21, 1999.
- Testimony before House Committee on Government Reform, "Narcotics Threat from Colombia," August 6 1999.
- Testimony before House Committee on Government Reform, "Oversight of U.S./Mexico Counternarcotics Efforts," March 4, 1999.
- Testimony before House Committee on International Relations, "Anti-Drug Effort in the Americas and the Implementation of the Western Hemisphere Drug Elimination Act," March 3, 1999.
- Testimony before Senate Caucus on International Narcotics Control, "*Drug Control: Update on U.S.-Mexican Counternarcotics Efforts*," February 24, 1999.
- Testimony before Senate Caucus on International Narcotics Control, "*U.S. Efforts in International Demand Reduction Programs*," June 18, 1998.
- Testimony before House Committee on International Relations, "*U.S. Narcotics Policy Towards Colombia*," March 31, 1998.
- Testimony before House Committee on Government Reform, "*Oversight of U.S./Mexico Drug Cooperation*," March 18, 1998.
- Statement before the House International Relations Committee on update of Counternarcotics Program in Colombia, March 1998.

To my best recollection, this is the complete list of speeches and testimonies I have given.

17. **Selection:**

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

I believe that I was nominated by the President because my 36-year professional career spent implementing, analyzing, and shaping national and homeland security has uniquely prepared me for the challenges facing DHS' National Protection and Programs Directorate (NPPD).

My career began in the field, serving first as a Marine in Vietnam, and later rising through the ranks of the Foreign Service and Civil Service. Having spent nearly 30 years on both the military and diplomatic front lines of the Cold War, I spent the following 15 years working on the prominent emerging threats facing the United States after the fall of the Soviet Union. I have served on the National Security Council Staff as a Director or Senior Director and Special Assistant to the President under the previous four Presidents on matters relating to counter-terrorism, counter-narcotics, and intelligence matters (1988-98, 2002-2003). I was the Assistant Secretary of State for International Narcotics and Law Enforcement Affairs (1998-2002); and I worked on national security affairs on the 2004 and 2008 Presidential campaigns and on the 2008-2009 Presidential transition. Between Mr. Schneider's resignation and Ms. Holl Lute's confirmation, I served as the Acting Deputy Secretary for Homeland Security.

During my career, I worked directly on such major national, international, and homeland security issues as:

- Middle East airplane high jackings in the mid-80s
- The Pan Am 103 bombing investigation
- UN sanctions on Libya
- Various aviation security reviews including those following the crashes of Pan Am 103 and TWA 800
- Post-9/11 aviation security measures and regional counter-terrorism programs for the Horn of Africa and Southeast Asia
- Plan Colombia
- Counter-narcotics assistance for Mexico
- Drug Kingpin legislation
- Counternarcotics programs in Afghanistan and Pakistan
- International law enforcement training around the world, including International Law Enforcement Academies in Budapest, Bangkok, San Salvador, and Roswell, New Mexico.

During the George W. Bush Administration, I worked with the Homeland Security Staff on a number of issues prior to the standup of the Department of Homeland Security, e.g., aviation security ranging from the first days of the Transportation Security Administration to the threat from shoulder-fired surface-to-air-missiles, and database and identity management.

I have dealt with budgets of over \$1 billion— both on budget preparations and implementation within various Administrations and on appropriations with the Hill since 1980 — including Security Assistance at the State Department, peacekeeping assistance at the NSC, and counter-narcotics assistance at the NSC and the State Department. I have also supervised the Bureau of International Narcotics and Law Enforcement Affairs (1998-2002), which numbered over 1000 personnel in Washington and in numerous embassies around the world.

With respect to specific issue areas under NPPD's purview, I began working on the first World Trade Center bombing when it was seen as both a physical and cyber security concern for critical infrastructure. I similarly worked on the Oklahoma City bombing. I was the NSC Staff lead for the Presidential (Marsh) Commission on Critical Infrastructure Protection, and I began the follow-on work on the first Presidential Decision Document on the subject (PDD 63). I have been a member of the Markle Foundation Task Force on National Security in the Information Age for the last four years. I have also worked on a wide range of homeland security issues at the National Security Network and co-chaired the Task Force that wrote *The Forgotten Homeland*.

NPPD is responsible for some of the most challenging vulnerabilities facing our nation today — such as cyber security, chemical security, and protecting critical infrastructure. If confirmed, I will dedicate myself to meeting these challenges, and I

believe that my nomination speaks to the confidence of the President and the Secretary that I can do so.

- (b) What do you believe in your background or employment experience affirmatively qualifies you for this particular appointment?
- See response to 17(a)

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?
 - I work at DHS and have no other business relations.
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.

In connection with the nomination process, I have consulted with the Office of Government Ethics and the Department of Homeland Security's designated agency ethics official to identify potential conflicts of interest. Any potential conflicts of interest will be resolved in accordance with the terms of an ethics agreement that I have entered into with the Department's designated agency ethics official.

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.

I have never been a registered lobbyist. As the President of the National Security Network, I provided information and analysis to Members of Congress and their staff.

During the Spring of 2007, I joined a national advocacy campaign to urge Congress to pass legislation restricting US troop presence in Iraq. My efforts in this effort were unpaid.

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.

While serving on the National Security Council in 1996, I received a preliminary briefing from the FBI that indicated the People's Republic of China may be attempting to influence certain U.S. congressional elections. Due to the preliminary nature of the briefing and the other pressing matters facing the NSC at the time, I did not immediately report this briefing to my superiors. Several months later, other developments put the issue of potential Chinese influence in U.S. elections in the national spotlight. I subsequently received a verbal reprimand from my superior at the National Security Council for failing to report the FBI briefing.

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.

- I was interviewed at some point in 2007 by the FBI in relation to the FBI investigation of the terrorist surveillance program. I have been told that I am not a target of the investigation.

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.

- In late 2001, I provided a sworn deposition in a civil proceeding concerning DynCorp, a firm contracted for aerial eradication in Colombia by the State Department Bureau for which I was the Assistant Secretary. The firm was being sued on behalf of several people in Ecuador who alleged that the spray had crossed into Ecuador and injured them. Several months later, I learned that a statement I had made in the deposition regarding a connection between FARC guerrillas in Colombia and Al Qaeda was incorrect. I had believed the statement was accurate at the time of the deposition. In 2002, upon learning the statement was incorrect, I issued a written statement regretting the inaccuracy.

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.)

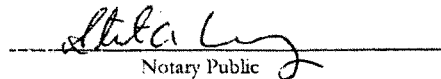
REDACTED

AFFIDAVIT

RAND BEERS 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 29th day of April, 2009


Notary Public

Stuart A. Connolly
Notary Public, District of Columbia
My Commission Expires 1/1/2012

**U.S. Senate Committee on Homeland Security and Governmental Affairs
Pre-hearing Questionnaire
For the Nomination of Rand Beers, to be
Under Secretary 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 I was nominated by the President because my 36-year professional career spent implementing, analyzing, and shaping national and homeland security has uniquely prepared me for the challenges facing DHS' National Protection and Programs Directorate (NPPD).

My career began in the field, serving first as a Marine in Vietnam, and later rising through the ranks of the Foreign Service and Civil Service. Having spent nearly 30 years on both the military and diplomatic front lines of the Cold War, I spent the following 15 years working on the prominent emerging threats facing the United States after the fall of the Soviet Union. I have served on the National Security Council Staff as a Director or Senior Director and Special Assistant to the President under the previous four Presidents on matters relating to counter-terrorism, counter-narcotics, and intelligence matters (1988-98, 2002-2003). I was the Assistant Secretary of State for International Narcotics and Law Enforcement Affairs (1998-2002); and I worked on national security affairs on the 2004 and 2008 Presidential campaigns and on the 2008-2009 Presidential transition. Between Mr. Schneider's resignation and Ms. Holl Lute's confirmation, I served as the Acting Deputy Secretary for Homeland Security.

During my career, I worked directly on such major national, international, and homeland security issues as:

- Middle East airplane high jackings in the mid-80s
- The Pan Am 103 bombing investigation
- UN sanctions on Libya
- Various aviation security reviews including those following the crashes of Pan Am 103 and TWA 800
- Post-9/11 aviation security measures and regional counter-terrorism programs for the Horn of Africa and Southeast Asia
- Plan Colombia
- Counter-narcotics assistance for Mexico
- Drug Kingpin legislation
- Counternarcotics programs in Afghanistan and Pakistan
- International law enforcement training around the world, including International Law Enforcement Academies in Budapest, Bangkok, San Salvador, and Roswell, New Mexico.

During the Bush Administration, I worked with the Homeland Security Staff on a number of issues prior to the standup of the Department of Homeland Security, e.g., aviation security ranging from the first days of the Transportation Security Administration to the threat from shoulder-fired surface-to-air-missiles, and database and identity management.

I have dealt with budgets of over \$1 billion— both on budget preparations and implementation within various Administrations and on appropriations with the Hill since 1980 – including Security Assistance at the State Department, peacekeeping assistance at the NSC, and counter-narcotics assistance at the NSC and the State Department. I have also supervised the Bureau of International Narcotics and Law Enforcement Affairs (1998-2002), which numbered over 1000 personnel in Washington and in numerous embassies around the world.

With respect to specific issue areas under NPPD's purview, I began working on the first World Trade Center bombing when it was seen as both a physical and cybersecurity concern for critical infrastructure. I similarly worked on the Oklahoma City bombing. I was the NSC Staff lead for the Presidential (Marsh) Commission on Critical Infrastructure Protection, and I began the follow-on work on the first Presidential Decision Document on the subject (PDD 63). I have been a member of the Markle Foundation Task Force on National Security in the Information Age for the last four years. I have also worked on a wide range of homeland security issues at the National Security Network and co-chaired the Task Force that wrote *The Forgotten Homeland*.

NPPD is responsible for some of the most challenging vulnerabilities facing our nation today – such as cybersecurity, chemical security, and protecting critical infrastructure. If confirmed, I will dedicate myself to meeting these challenges, and I believe that my nomination speaks to the confidence of the President and the Secretary that I can do so.

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 NPPD?

See response for question 1.

4. Have you made any commitments with respect to the policies and principles you will attempt to implement as Under Secretary for NPPD? 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.

I have recused myself from any dealings with Good Harbor Consulting and the National Security Network.

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.

7. In your responses to the biographical questionnaire, you stated that while working as the senior director for intelligence programs for the National Security Council you received a briefing from the FBI in 1996 indicating that China might be attempting to influence certain U.S. Congressional elections, but that you did not immediately report this information to your superiors due its preliminary nature and the other pressing matters facing the NSC at that time. Please provide a more detailed explanation and timeline of this incident, including a summary of who was present, what you were told regarding both the matter itself and with whom you could share the information, why you did not immediately inform your superiors what you had learned, what other actions you took and/or believed were necessary based on the information conveyed, when your supervisors learned of the briefing, whether you received subsequent briefings on the matter, and the timing and substance of the verbal reprimand.

I was the Senior Director for Intelligence Programs at the NSC from 1995 to 1998. A regular part of my duties was to be briefed by the FBI about counterintelligence cases. The timing of the FBI Chinese espionage briefing was the summer of 1996. The briefing was oral. My FBI assistant also attended. Two FBI counterintelligence agents provided the briefing. The essence of the briefing was that Chinese intelligence operatives were interested in gaining influence through political contributions. The details of the briefing were classified. The content indicated a case which appeared to be in the very early stages and I asked to be kept informed. As a result of the preliminary nature of the case, I did not feel there was enough useful information to brief the National Security Advisor, Tony Lake, at that time.

Following the 1996 election and the controversy surrounding possible Chinese contributions to the Clinton-Gore campaign, this briefing became public. As the White House conducted an inquiry into the briefing, my assistant indicated that he had remembered being told that we were not to brief our superiors and that version of the briefing became public. When the FBI became aware of that version of the briefing they denied that was the case. My own personal recollection which I stated during the inquiry

was that I did not remember such a restriction and that I would have disregarded it if I had felt the need to brief the National Security Advisor. Following the completion of the inquiry, I was verbally reprimanded by the new National Security Advisor Sandy Berger in early 1997, following Tony Lake's withdrawal of his nomination for CIA Director.

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

8. Why do you wish to serve as Under Secretary for NPPD?

NPPD's mission encompasses some of the most significant issues related to the safety and security of the nation and its citizens, including the defense of our nation's cyberspace, the protection of the critical infrastructure and key resources, and the securing of our borders by tracking the entrance and exit of foreign travelers. These mission areas pose significant challenges for which my 36 years of professional experience has well prepared me. If confirmed, I will tackle these challenges to the best of my abilities.

9. For the past few months, you served as the Acting Deputy Secretary of the Department of Homeland Security ("DHS" or "the Department") giving you a unique view into all components of DHS. What did you learn during that time that you intend to apply as Under Secretary of NPPD?

As Acting Deputy Secretary I had broad perspective of the Department and gained a detailed understanding of its mission areas, the relationship between the various components, and of its inner workings. As Under Secretary, I would leverage this knowledge and experience to ensure that NPPD was closely aligned with overall Departmental policies and priorities and to more effectively advocate for NPPD.

10. The Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act) eliminated the Preparedness Directorate and merged the Department's preparedness functions with the response and recovery functions in FEMA to create a new, revitalized FEMA. In the wake of this statutory reorganization, the Department created NPPD to house some of the remaining components of the earlier Preparedness Directorate as well as some other new and existing offices. Thus, the Directorate currently encompasses a disparate set of functions, ranging from infrastructure protection to emergency communications to US-VISIT to risk analysis and management to cybersecurity.

- a. What do you see as the Directorate's overarching mission?

I see the Directorate's overarching mission to be the mitigation of risk to the nation and its citizens; the risk to the nation's critical infrastructure by manmade or natural disasters; the risk to the country's cyberspace by cyber criminals and nation states; and the risk of individuals entering into this country with the intent to do harm.

- b. What do you see as the NPPD's strengths and weaknesses in its ability to accomplish this mission?

NPPD has number of strengthens that support it ability to accomplish it mission. Most important of these is the overall quality of its employees, who are experts in their respective fields and work incredibly hard on daily basis to ensure that NPPD is successful. However, NPPD faces several challenges. The most significant being NPPD's ability to hire an ever increasing number of employees to meet the demand of its rapidly growing components. A further challenge is acquiring the necessary facilities to house the growing size of its components and to consolidate these facilities in a way to allow NPPD to more effectively carry out its mission.

- c. Do you think the current organization of NPPD continues to make sense?

I believe that NPPD's organization structure allows it to accomplish its current missions. However, if confirmed, I intend review the Directorate's organizational structure to identify potential improvements to gain greater efficiencies.

- d. Are there changes to the scope or structure of the Directorate that you would recommend?

I am in the process of reviewing the overall structure and scope of the Directorate and not yet able to provide any definitive conclusions. However, if confirmed, I will review the structure of the Directorate to determine if improvements can be made. I look forward to working with the Committee on this issue. That said, there are two organizational changes that are called for in the FY 2010 President's budget request: moving IGP out of NPPD and moving FPS into NPPD.

- e. How does NPPD complement the missions of other DHS functions?

NPPD complements other DHS functions very well. For example, NPPD's Office of Infrastructure Protection coordinates with FEMA and the DHS Office of Operations during a response to a disaster, providing information regarding critical infrastructure and acting as a point-of-contact with the private sector owners to help recovery efforts. Further, NPPD's US-VISIT program provides its biometric database, IDENT, to CBP and even the U.S. Coast Guard to help identify potentially dangerous individuals as they enter the country.

11. In his March 5, 2009, resignation letter to Secretary Napolitano, former Director of the National Cybersecurity Center Rob Beckstrom referenced a plan to move NPPD to an NSA facility at Fort Meade. Are you aware of any plans to physically move the Directorate or any part of the Directorate to NSA facilities?

The Department has examined a number of potential options for meeting the growing facilities requirement of the Office of Cybersecurity and Communication (CS&C).

NPPD is currently implementing a short- to mid-term facilities plan that will consolidate the majority of CS&C in the Ballston area. The Department is in the process of developing a long-term facilities plan for CS&C and a move to Fort Meade was an option in the previous Administration; however, no final determination has been made as to where CS&C will be physically located in the long-term.

12. On March 11, 2009, Secretary Napolitano named Philip Reitingger to be Deputy Undersecretary of NPPD. The press release indicated that Mr. Reitingger's principal responsibility would be cybersecurity stating, "Reitingger will be charged with protecting the U.S. government's computing systems from domestic and foreign threats."
 - a. What is your understanding of your respective roles?

If confirmed as Under Secretary, I will be responsible for providing overall leadership to NPPD and setting Directorate policies and priorities. The Deputy Under Secretary, Philip Reitingger, comes to the Department with broad experience in cybersecurity. As my deputy he will be primarily responsible for overseeing the Department's cybersecurity efforts. He will also assist me in the day-to-day management of NPPD.
 - b. What will be the reporting structure?

If I am confirmed as Under Secretary, Mr. Reitingger will report directly to me.
 - c. Will Mr. Reitingger have responsibility for any NPPD issues other than cybersecurity?

In addition to Mr. Reitingger's primary cybersecurity duties, he will be responsible for assisting me in the management of NPPD, including helping set strategic direction, building NPPD's organizational capabilities, and overseeing the significant expansion of NPPD components.
 - d. How will his responsibilities interact with those charged to the Assistant Secretary for Cybersecurity and Communications?

Mr. Reitingger will have overall responsibility for the strategic direction of DHS' cybersecurity efforts. The Assistant Secretary of Cybersecurity and Communications (CS&C) will support Mr. Reitingger but will also oversee the day-to-day operations of CS&C.
13. If confirmed, what would be your top priorities? What do you hope to have accomplished at the end of your tenure?

I believe that NPPD is responsible for some of the most difficult challenges facing our Nation. If confirmed, my priorities would be to:

 - Continue building NPPD's capabilities to defend the nation's cyberspace.
 - Continue to increase the security of the country's chemical facilities by building a strong Chemical Facilities Anti-Terrorism Standards (CFATS) program.

- Strengthen our private sector partnerships to allow for increased information sharing and coordination between the federal government and private industry regarding the protection of critical infrastructure and key resources.
- Secure our nation's borders by implementing an effective Air Entrance and Exit solution.

III. Policy Questions

Management

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

I believe that the three major elements of good management are:

- selection, training, and career development of personnel;
- empowering staff to take initiative; and
- providing clear guidance and feed back to ensure proper direction and course corrections when necessary.

15. NPPD has a large number of vacant positions due to both significant growth in the responsibilities and budget of certain programs within the Directorate, such as cybersecurity and chemical security, and to challenges in attracting, hiring, and retaining qualified personnel. In 2008, NPPD established a dedicated hiring team within the Directorate to help expedite the hiring process.

- a. How do you intend to address the large numbers of vacancies in NPPD?

Based on my interactions with NPPD leadership, I understand that this is a priority for the Directorate and it will be a priority of mine if I am confirmed.

It is my understanding that at the beginning of FY 2008 there were 491 employees within NPPD. Nine months later the total workforce had only had a net gain of two, after you offset the number hired by the number of attritions. At that same time NPPD contracted with Booz, Allen Hamilton (BAH) and brought on board two very seasoned professionals to serve in the capacity of Director of Resource Administration and Human Capital Officer. Under their direction, over the course of the next 10 months, the NPPD workforce has grown to 780. While this is a noteworthy improvement, there are significant challenges that continue to be addressed in order to accomplish NPPD's hiring commitment. It is my understanding that NPPD intends to address the remaining large number of vacancies through a multi-pronged approach.

The NPPD Resource Administration leadership has conducted a comprehensive review of the entire hiring process over the past 6 months in order to identify those aspects that could be streamlined or improved. A number of steps are being

undertaken as a result of that analysis including: streamlining aspects of the current security process; utilizing more cost efficient staffing services available through OPM; enhancing partnership with the CHCO's office; hiring experienced federal HR staff; as well as exploring the possibility of requesting delegated personnel authorities similar to the non-HQ DHS components in order to improve efficiency. Employing these changes in coordination with an aggressive hiring strategy within each of the NPPD components should enable the directorate to make significant progress towards accomplishing these goals.

- b. Do you believe you need direct hire authority for certain positions within the Directorate in order to hiring qualified staff in a timely manner?

NPPD is currently reviewing ways to increase the efficiency of its hiring process to bring on qualified staff in a timely manner. This may include requesting that NPPD be granted direct hire authority or that NPPD be delegated broader personnel authorities.

16. Contractors are prohibited by law from performing "inherently governmental functions." However, various sources define "inherently governmental" differently and, in any event, it is not unusual for government contractors to provide services that, even if they do not technically meet the definition, closely support "inherently governmental functions." The Committee, the Government Accountability Office (GAO), and many outside observers recognized the need for DHS's heavy reliance on contractors during its early days, given the need for DHS to attain specific expertise quickly. More than six years later, many offices remain heavily staffed by contractors who perform a variety of tasks at the core of DHS's operations, including policy planning, the drafting of regulations, intelligence analysis, and preparation of budget requests.

- a. What will you do to strengthen NPPD's own ability to perform those tasks at the core of its operations, whether inherently governmental or closely supportive of "inherently governmental functions?"

If confirmed, I will work to identify and reduce the number of contractors that perform "nearly inherently governmental functions" by hiring additional government personnel. Some of the areas that I will pursue will be as follows: Human Capital, Budget and Financial Operations and Procurement. This will require the reprogramming of funds and the increase in the numbers of government positions allocated to NPPD.

- b. Given the government's extensive reliance on contractors, what would you suggest are the key considerations in determining the appropriate role for contractors in supporting government operations (particularly, in the areas that border on "inherently governmental functions," such as rulemaking or determining agency policy)?

I believe that the key considerations in determining the appropriate role for contractors in supporting government operations is the determination whether the activity requires the exercise of substantial discretion (decision making and/or signature authority). Otherwise, if the service is listed in the "yellow pages," it is probably not inherently governmental.

Therefore, rulemaking and the determination of the agency policy should be considered inherently governmental functions. I do not believe that "fact-gathering" and analysis in support of those areas are inherently governmental; however, oversight of those functions is a government function. Moreover, it is my general intention to replace as many contractors as possible as quickly as possible.

- c. Government contractor employees often work side-by-side with federal employees, and also perform the same or similar functions as their federal employee counterparts. Please discuss any experiences that you have had managing such augmented workforce and your views on ensuring that government agencies establish appropriate safeguards to prevent conflicts of interest by contractor employees?

During my time as Assistant Secretary of State for International Narcotics and Law Enforcement Affairs I had contractors who worked in the areas of aviation, training, and recruitment. My personal opinion based on this experience is that contractors provide a service but must be closely supervised to ensure that their actions represent the U.S. government and comply with our laws and procedures. Moreover, we must keep basic distinctions between government employees and contractors. I believe that contractors should perform tasks as assigned and should not be required to exercise substantial discretion (decision making and/or signature authority).

- d. Do you believe that contracting out work, even if not "inherently governmental," can reduce essential staff expertise or otherwise diminish the institutional strength of agencies? If so, how should such considerations be taken into account in determining whether work should be contracted out or done in-house?

Yes, I believe that contracting can reduce essential staff expertise or otherwise diminish the institutional strength of agencies if not managed properly. If managed properly, contracting can expand essential staff expertise or otherwise improve the institutional strength of agencies. Specifically, if contractors are limited to advisory functions they should serve as force multipliers allowing the government to concentrate in more important tasks.

Proper management of contractor support requires limiting contractors to administrative and advisory functions. At the same time government personnel should be required to remain as task lead and be responsible for the work performed.

17. The previous NPPD Under Secretary committed at his confirmation hearing to try to reduce the Directorate's over-reliance on contractors by converting contractors

performing inherently governmental functions to federal positions. Is this a policy you intend to continue?

Yes. If confirmed, I will work to more broadly replace contractors as well.

Critical Infrastructure Protection

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

Achieving protection and resiliency across all 18 critical infrastructure and key resources (CIKR) sectors from man-made events (accidents, terrorism) and natural hazards is a complex challenge because of the diversity of the sectors, the fact that the majority of the mission is accomplished through voluntary rather than regulatory relationships, and the dynamic risk environment. The Office of Infrastructure Protection (IP) and its Federal, regional, State, local, territorial, tribal, and private sector partners developed and are implementing the National Infrastructure Protection Plan (NIPP). Using the NIPP as its guide, IP leads the coordinated national effort to reduce risk to the Nation's CIKR and to enable national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.

The President's National Infrastructure Advisory Council (NIAC), in its 2008 report, *Critical Infrastructure Partnership Strategic Assessment*, concluded that the public-private sector partnership represents the best long-term strategy to secure the Nation's CIKR. IP has forged strong, effective relationships with stakeholders at all levels that continue to mature and enhance protection and resiliency. Currently, IP is focused on expanding partnership efforts to the next level with State, territorial, tribal and local jurisdictions, regional coalitions, and State and local fusion centers, providing them with capabilities and tools to develop critical infrastructure protection programs, and ensuring NIPP implementation at those levels. Challenges to address as we move into the future include sustaining the robustness of the partnership among all stakeholders, and addressing the aging of key CIKR assets and systems throughout the country. If confirmed, I will work to meet those challenges.

19. Ensuring the security of the nation's most critical infrastructure and key resources is a vital mission of the Department. In 2003, former President Bush issued Homeland Security Presidential Directive (HSPD) 7 (Critical Infrastructure Identification, Prioritization, and Protection) to coordinate federal infrastructure protection responsibilities, directing the Secretary of Homeland Security to lead these efforts. HSPD-7 tasked the Secretary of Homeland Security with developing the National Infrastructure Protection Plan (NIPP) and encouraged the Department and sector-specific agencies to develop voluntary private-public structures, such as the private sector and government coordinating councils, to set national priorities for, and provide a coordinated approach to, critical infrastructure and key resources protection.

- a. What role do you believe DHS should play in critical infrastructure protection within the federal government?

I firmly believe that DHS must continue to fill its crucial role in leading our Nation's efforts for critical infrastructure and key resource (CIKR) protection. In addition to HSPD-7, DHS' efforts are also based on the Homeland Security Act of 2002 which establishes DHS' responsibilities and authorities for the protection of the Nation's CIKR. It assigns DHS responsibility for ensuring the NIPP's implementation, and recommending the "measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies and authorities, the private sector and other entities."

Do you believe this role differs from the direction provided under HSPD-7?

No, I think they are aligned. HSPD-7 designates the Secretary of DHS as the principal Federal official to lead CIKR protection efforts among Federal departments and agencies, State and local governments, and the private sector and provides additional clarity to the 2002 Act. Under the direction of HSPD-7, the National Infrastructure Protection Plan was developed and issued; it delineates the roles and responsibilities of DHS and the 18 Sector Specific Agencies (SSAs), in carrying out CIKR protection activities while respecting and integrating the authorities, jurisdiction, and prerogatives of these and other partners.

What relationship do you believe DHS should have with sector-specific agencies?

It is my understanding that DHS has established solid relations with the SSAs. As set out in the NIPP, the enormity and complexity of the Nation's CIKR, the distributed character of our national protective architecture, and the uncertain nature of terrorists, manmade or natural hazards, make effective implementation of protection and resiliency efforts a great challenge. Successful protection and resiliency efforts can only be achieved through active collaboration, coordination and information sharing with the SSAs; and must also include State, local, tribal and territorial representatives at all levels, and private sector owners and operators.

Do you believe this relationship can be strengthened, if so, how?

The bedrock of any relationship is trusted, honest communication, and the NIPP affords us the established processes and mechanisms to foster such communication. Therefore, I believe that strengthening the relationship with the SSAs, and all of our public and private sector partners, simply requires a sincere, ongoing commitment to what we have already built together.

If confirmed I will work with the Office of Infrastructure Protection to review the current relationship and determine if there are additional mechanisms that could be employed to further strengthen our relationship with the SSAs. Based on the ongoing DHS focus on

the spread of the H1N1 influenza, I believe that more planning on continuity of business applications in such a scenario is an important task ahead.

b. What is your view of the NIPP and the sector-specific plans developed in association with the NIPP?

I believe it is important to continue to build on existing structures and lessons learned but make sure these structures are used to drive measurable improvements in security. The NIPP is our national strategy for CIKR protection and resiliency, and its implementation to date clearly demonstrates what we have been able to achieve through partnership building and information sharing. The NIPP is the framework for how the 18 sectors will prioritize their CIKR and resiliency initiatives while building on public and private sector protective strategies to allow for a partnership that will further fortify these national assets. It provides the overarching approach for integrating the Nation's many CIKR protection initiatives into a single national effort. Because of the unique and individual needs of each sector, developing a generalized risk management strategy would be ineffective. Sector Specific Plans (SSP) provide that next step which is an exclusive snapshot of the sector profiles, partners, security goals as well as infrastructure prioritization methodologies. The SSPs are a direct result of the collaboration between both public and private sector representatives at all levels and permit DHS and the SSAs to fully identify risk and threat landscapes of each sector while coordinating with security partners to mitigate these issues.

Do you intend to make significant changes to these documents?

It is my understanding that the updated version of the NIPP, "Partnering to Enhance Protection and Resiliency," was reviewed, revised and reissued earlier this year. Currently, the SSAs are involved in their SSP triennial review and rewrite process, in collaboration with DHS, with their expected reissue in 2010. The Department anticipates the SSPs to reflect the maturation of the sectors, protection and resiliency programs and initiatives, and information sharing mechanisms that has taken place since their first release in May of 2007.

If confirmed, I will review the SSP guidance and the response documents to make sure they work towards the Department's goal of improving the security of our Nation's critical infrastructure/ key resources.

How would you make these documents more proactive and actionable?

As I noted previously, an updated version of the NIPP was reviewed and reissued in 2009, and the triennial review and reissue of the SSPs is currently underway. As a national-level plan, the NIPP establishes the framework for the implementation of actionable CIKR protection and resiliency efforts. It also codifies many of the mechanisms utilized for information sharing and during all-hazards incident management activities. Therefore, the NIPP enables a broad spectrum of proactive and reactive CIKR capabilities and actions. I believe the SSPs are continuing to

mature in their comprehensiveness, as a direct result of the ongoing efforts of the SSAs and their State, local, regional, and private sector partners. During this maturation process, through ongoing engagement by DHS, we will encourage all stakeholders to further clarify goals and objectives, and actively approach the measurement of their programmatic effectiveness.

- c. What is your view on voluntary private-public partnerships as a tool to ensure the security of our nation's critical infrastructure and key resources?

Voluntary private-public partnerships are an important tool for the Department to use when interfacing with the private sector, given that the private sector owns much of the Nation's critical infrastructure. The benefits derived from voluntary private sector engagement have assisted in the creation of information sharing environments and security enhancement products that otherwise could not have been achieved. Support through the partnership model brings representatives from all CIKR sectors to participate in a wide range of critical infrastructure activities. Government programs are informed by CIKR sector councils with valuable industry knowledge. This interaction provides the government with the information necessary to produce effective planning tools, programs and deployment of resources.

Do you believe the current model utilizing Sector Coordinating Councils, Government Coordinating Councils, and Information Sharing and Analysis Councils is an effective framework?

Yes, I believe that the structure provides a trusted environment for the engagement and exchange of information between the Government and the owners and operators of the nation's critical infrastructure. Additional evidence of the councils' value and effectiveness is demonstrated by the formation of similar partnership frameworks at the state and local levels. The Sector Specific Coordinating Councils, Government Coordinating Councils and Information Sharing and Analysis Centers are vital to continued effective collaboration with our CIKR partners.

During significant incidents, the partnership framework provides an essential mechanism to enable free flow of information between the Government and the owners and operators of our Nation's CIKR. This information flow assists CIKR decision-makers in executing their business continuity and recovery plans while simultaneously ensuring that all levels of government are aware of and able to respond to critical issues faced by CIKR owners and operators. This promotes greater resiliency by ensuring that decisions affecting and affected by CIKR status are carefully considered, and all available information is used to make the best decisions to protect and restore essential critical infrastructure.

That said, if confirmed, I will look closely at this framework to ensure that it is fully effective.

- d. What actions as Under Secretary would you take to develop and improve voluntary

public-private programs?

If confirmed, I will work with our Federal, State and local, and private sector partners to identify where any gaps may exist in our current programs. A high priority will be to develop an understanding of what if any changes are occurring at the State and local level and within the private sector regarding infrastructure protection and resiliency efforts and spending given the current economic condition. Continuity of operations plans will be an important area for review.

20. Voluntary relationships are not always enough to secure critical infrastructure and protect the American people. For this reason, Congress has authorized various federal agencies to regulate the activities of select sectors, such as the chemical, nuclear, and transportation sectors. However, the majority of critical infrastructure sectors are not subject to federal security regulation.

- a. How do you respond to concerns that the private sector, which owns at least 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?

There cannot be a one-size-fits-all approach to CIKR protection, which is often the outcome of a rigid regulatory framework. I think that effective infrastructure protection must be built on a combination of considerations that reflects an understanding of vulnerabilities, interdependencies, and priorities in the all-hazards context. The diversity of the CIKR sectors means that different types of protection activities may be the most effective for the unique circumstance of an individual facility or system. The owners and operators of the nation's infrastructure, whether they are in the private sector or the public sector, have a vested interest in and responsibility to ensure that their assets, systems or networks are protected to a level commensurate with the risk they face.

- b. How can DHS better leverage existing regulatory entities not currently focused on security, but that have long-standing relationships and in-depth familiarity with the sectors that they oversee?

DHS maintains robust relationships with a number of agencies with regulatory authority outside the security domain. We will continue to actively engage the full spectrum of these agencies and organizations that have ongoing relationships and interactions with our CIKR partners.

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

As I stated, regulation should be applied where risk and consequences are the greatest, and should be outcomes-based. At this point, it would be premature for me to offer an opinion on this subject. If confirmed, I will ensure that NPPD continues to

work with all of its partners to identify any gaps that exist with regard to high risk and high consequence assets and systems and takes the appropriate actions to close those gaps.

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

I believe that the consideration of additional regulatory authorities for the Department would require the involvement of Congress.

21. The Office of Infrastructure Protection (OIP) initially focused its activities on protecting rather than ensuring the resiliency of our nation's critical infrastructure and key resources. Last year the Homeland Security Advisory Council recommended refocusing the Department's critical infrastructure and key resources protection activities on resiliency as a top priority for the next Secretary because "we cannot protect everything, against all things, at all times, and at all costs." Some experts have also argued that the private sector is more open to the concept of resiliency than protection because the business case for investing in resiliency is more compelling.

- a. What role do you believe resiliency should have in the Department's critical infrastructure and key resources activities?

I believe that resiliency is an essential element of ensuring that the critical goods and services provided by the nation's infrastructure can continue to be provided to the nation in a sustained manner. The 2009 NIPP, subtitled "Partnering to Enhance Protection and Resiliency," not only provides the baseline for DHS infrastructure protection guidance, but more significantly it sets the tone for the Department's commitment to resiliency and further outlines how the concepts of protection and resiliency are interlinked. Certain sectors are more likely to embrace resiliency given their inherent operational characteristics, while others may focus more on specific types of physical protection or training or rapid response to reduce risk and minimize consequences.

- b. What are your views regarding the appropriate balance between protection and resiliency?

Protection depends on an overarching risk-management strategy that fully acknowledges and supports the concept of resiliency where it offers the best solution to managing a particular risk or set of risks.

Since 9/11, significant efforts have been underway to define the scope of work required to establish the processes and mechanisms to secure and mitigate the vulnerability and ensure the functionality of CIKR across our country. The private sector has made substantial investments to boost resiliency, increase redundancy, and develop contingency plans. To support these efforts, the Department has provided

significant amounts of risk-based grant funding to deter threats, reduce vulnerabilities, and build resiliency.

Because the private sector owns and operates most of the Nation's critical infrastructure, DHS has pursued a voluntary partnership approach, where government and the private sector work together under a common framework to set goals and priorities, identify key assets, assign roles and responsibilities, allocate resources, and measure progress against national priorities. As important as resiliency is to a number of our critical sectors, adopting a "one size fits all" solution could create an imbalance. The chemical, nuclear and energy sectors are prime examples of the need to balance our concerns about infrastructure restoration after an incident, with our ability to prevent the release of dangerous substances into populated areas. Preventing the loss of human life must remain our number one goal.

c. How would you encourage resiliency throughout the private sector?

I think that protecting and ensuring the resiliency of the nation's infrastructure requires a wide range of activities. There cannot be a single common approach to CIKR protection and resiliency, this requires that DHS work with a variety of partners in a dynamic risk landscape to prioritize activities and devise a strategy based on a combination of considerations that reflect an understanding of vulnerabilities and interdependencies in the all hazards context. The NIPP and its supporting SSPs chart the path for continuous improvement of security and resiliency of our critical infrastructures, and the focused activities of IP in concert with all of our CIKR partners ensures their preparedness. Furthermore, participation in the Voluntary Private Sector preparedness Standards Program (PS-Prep) will make a significant enhancement in the preparedness and resiliency of the nation's critical infrastructure.

22. After finding a large majority of the private sector was unprepared for a terrorist attack, the 9-11 Commission recommended that the federal government promote a preparedness standard for the private sector. To this end, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Recommendation Act) (P.L. 110-53) established the Voluntary Private Sector Preparedness Accreditation and Certification Program within DHS, which will allow interested private sector companies to be certified as complying with voluntary preparedness standards. Former Secretary Michael Chertoff gave FEMA the lead responsibility for managing the program, and the Office of Infrastructure Protection is among the components working closely with FEMA on the program. The deadlines in the statute for developing and implementing the program have passed, but the program is not yet fully implemented.

a. Do you believe DHS has a responsibility to encourage private sector preparedness?

Yes, I believe that DHS has a responsibility, but it is a shared responsibility as the private sector owns and operates most of the essential functions and services in communities: therefore, a high level of private sector preparedness is essential to both

the nation and to individual communities. We must work with our state, local, and private sector partners, as well as other federal entities in creating a culture of preparedness. Improved private sector preparedness is needed to meet the wide range of disruptive challenges that may occur. Evidence and intuition suggests that the better prepared the private sector is, especially the nation's critical infrastructure, the earlier it can recover and resume operating after a disruption, reducing the impacts to the nation and to local communities. Our current activities associated with the H1N1 influenza outbreak are a clear indication that more work is needed.

- b. Do you believe OIP should continue to play a leadership role in the implementation of the Voluntary Private Sector Preparedness Accreditation and Certification Program? Will you make quickly implementing the program a priority?

I think that the public-private partnership framework under the NIPP has been a success and has significantly improved the protection of our nation's critical infrastructure. The program has the potential to make additional significant contributions to the preparedness and resilience of the country's critical infrastructure. I understand that FEMA has the lead for the program, and IP's leadership and contributions have been instrumental in the development of the program. As the 18 CIKR sectors will be key participants in the program, IP must remain engaged in the development and implementation of the program, especially as it relates to those 18 CIKR sectors. From the critical infrastructure perspective, it is important that the program is implemented in a way that recognizes and takes into account the regulations, best practices and, other ongoing activities that already contribute to preparedness in the critical infrastructure sectors. IP will work with each of the CIKR sectors to identify those existing laws, regulations, and sector best practices, and develop a framework for applying DHS-adopted voluntary preparedness standards to the individual sectors in ways that make sense for each.

- c. During the development of the Voluntary Private Sector Preparedness Accreditation and Certification Program, some expressed concern that the views of smaller private sector companies are not adequately being taken into account. Will you commit to working to ensure that the program meets the statute's requirements for small business concerns?

As noted previously, FEMA is the lead for this program. However, if confirmed, I will work with the Office of Infrastructure Protection to ensure the concerns of small businesses are considered.

23. The Department's Office for Bombing Prevention (OBP), located within the Office of Infrastructure Protection, leads the Department's efforts to deter, detect, prevent, protect against, and respond to terrorist improvised explosive device (IED) threats. OBP is also the Department's lead for coordinating DHS' roles and responsibilities as assigned by HSPD-19 implementation plan. OBP also provides a number of services on behalf of OIP such as grant support and infrastructure protection training courses to private sector

personnel and state and local officials. In November 2007, the Committee approved a bill, the National Bombing Prevention Act of 2007 (S. 2292) to codify the existence of this office within OIP and strengthen the authority and budget of this critical office.

a. Do you support the mission of the Office for Bombing Prevention?

Yes, I support the mission of OBP which serves as DHS' focal point for strategic planning, coordination, capacity building, and information sharing in the effort to improve bombing prevention activities throughout the Federal government, State and local jurisdictions, and the private sector as outlined in Homeland Security Presidential Directive-19 (HSPD-19) and associated Implementation Plan (IPLAN). OBP provides national leadership to coordinate programs and improve capabilities that address the threat of bombing attacks targeting CIKR and public gathering places. If confirmed, I will continue the focus on successful implementation of the IPLAN.

b. Do you agree that OIP is the appropriate place for OBP within the Department?

Yes, I believe that NPPD/IP is the appropriate location for OBP. Through NPPD/IP, OBP leverages key initiatives to assist with the Department's unique responsibilities to counter terrorist use of explosives through preparedness activities, infrastructure protection, information sharing, capabilities analysis and enhancement, public awareness, and outreach to the private sector.

c. Historically OBP's budget and staffing levels have been relatively small in comparison to its significant mission. S.2292 called for an annual budget of \$25 million to appropriately support OBP's important missions. Will you commit to properly support OBP and advocate for increase funding and staffing levels?

The FY 2010 budget request is \$14.2M, which is an increase of \$4M from the FY 2009 enacted funding. This enhancement will allow for the completion of 16 of 22 HSPD-19 Implementation Plan recommendations that are the responsibility of DHS, increased capability assessments of bombing prevention capabilities across the country, and increased bombing prevention information services for Federal, State, local and private sectors.

24. OIP is also responsible for managing the Protective Security Advisor (PSA) program. PSAs are located in communities throughout the country to assist and support local community and business efforts to protect critical infrastructure and further State and local homeland security initiatives. As DHS's infrastructure representatives in the field, PSAs regularly interact with State Homeland Security Advisors, emergency managers, private sector owners and operators of infrastructure, local representatives of other DHS components and federal agencies, neighboring States, territorial, and tribal entities. What is your view of the PSA program and do you believe it needs to be strengthened? If so, how will you strengthen it?

I believe that the PSA Program has proven to be of considerable value to our Federal, State, local and owner/operator CIKR partners nationwide.. There are currently 86 PSAs deployed to 50 States and 1 Territory. The PSAs serve as liaisons between DHS, the private sector, and Federal, State, territorial, local, and tribal entities; and serve as the DHS onsite critical infrastructure and vulnerability assessment specialists. During natural disasters and contingency events, PSAs work in State and local Emergency Operations Centers, and the Joint Field Office (JFO) if established and provide expertise and support to the IP Infrastructure Liaison Cell, working to support the Principal Federal Official (PFO) and Federal Coordinating Officer (FCO) responsible for domestic incident management. Additionally, PSAs provide support to officials responsible for special events planning and exercises, and provide real-time information on facility criticality and recommended protective measures to facility owners and operators, and State and local representatives. If confirmed, I will work to ensure that the PSA program is fully staffed and funded.

Cybersecurity

25. NPPD includes the Office of Cybersecurity and Communications (CS&C), which has broad responsibilities for protecting our communications and cyber infrastructure. As you know, for years there have been significant vulnerabilities in these networks. Vulnerabilities have led to massive identity theft, monetary loss, and leaks of classified information, and have had an effect on all levels of government and throughout industry. Additionally, cyber threats to Supervisory Control and Data Acquisition (SCADA) systems – which control industrial processes – have the potential to cause devastating impacts on critical infrastructure, including the electric grid and the water supply.

- a. Please discuss your familiarity and experience with cybersecurity issues.

During my time on the NSC Staff, I worked on a variety of cyber related issues. As indicated earlier, they included supervision of the Presidential (Marsh) Commission on the Protection of Critical Infrastructure and direction of the initial drafting of PDD 63, the first major Presidential decision concerning cybersecurity. As Assistant Secretary of State for International Law Enforcement Affairs I led delegation to Canada and the UK to discuss cybersecurity. In addition, I worked with Richard Clarke in directing the task force which produced The Forgotten Homeland and the chapter on cybersecurity and have discussed cyber issues on a regular basis with Clarke from the time I handed off PDD 63 until the present. While I am not a technologist, I believe that my early and continued involvement in the subject give me a detailed knowledge of the associated public policy issues, ranging from privacy concerns to the role and limitations of the intelligence community to the need for clear direction from a central authority and the need to breakdown barriers in the establishment of an effective cybersecurity regime.

- b. If confirmed, what steps do you intend to take to improve the nation's cybersecurity, both with respect to the government and private networks?

Cybersecurity is one of the most serious challenges we face. Information networks are vital to our economic and national security. This is a significant undertaking, and one where I understand that DHS has taken important steps that create the foundation for a more secure cyber infrastructure for government and the critical infrastructure. I intend to build upon DHS's efforts with respect to the Comprehensive National Cybersecurity Initiative. Significant work has been done to assist Agencies consolidate and reduce their Internet access points; to develop and deploy intrusion detection systems; and to prepare for deployment of intrusion prevention systems. DHS must look at current strategies to see if they remain effective and efficient across the civilian executive branch departments and agencies. DHS must also continue to recruit and retain the right work force, and I will work to lead that effort.

DHS must also continue to work closely with the private sector to identify appropriate roles and responsibilities for securing private sector networks and cyber infrastructure. If confirmed, I will work with the Interagency and the private sector to determine how we can best assist the private sector and determine if DHS has the right capacity, capability and authority to help the private sector secure its infrastructure.

- c. Given the respective roles of the Office of Management and Budget, the Department of Defense, the National Security Agency and other agencies, what do you believe to be the role of DHS with regard to cybersecurity?

DHS is the lead agency in coordinating the security of Federal Civil Executive Branch networks and working with owners and operators of critical infrastructure and key resources (CIKR) sector to defend their networks. It works with the private sector, academia, and Federal, State, local, tribal and international governments to assess and mitigate cyber risk and prepare for, prevent, and respond to cyber incidents. In executing its cybersecurity missions, DHS encounters common threats and vulnerabilities to government, public and private sector critical information infrastructure and is establishing processes and coordination mechanisms to share that information to assist non governmental entities defend their networks.

- d. Do you believe additional federal regulation or enhanced private sector cooperation is needed to ensure that private sector companies act to protect critical cyber infrastructure?

While the security of our nation's critical infrastructure networks is vital to our national and economic security, if it is determined that any new regulation is required, it must be carefully crafted to avoid unintended consequences. Poorly developed regulations could have a damaging effect on our economy or result in a situation where established standards are viewed and implemented by industry as a "maximum" rather than a "minimum" level of security.

However, regardless of possibility of new regulations, DHS must continue to enhance its private sector cooperation. We frequently hear the figure that 85% of the nation's critical infrastructure is owned and operated by the private sector. Because the government does not own and operate cyberspace, DHS absolutely must continue to build on and improve its partnership with industry. The National Infrastructure Protection Plan framework and coordinating bodies like the IT Sector Coordinating Council and the Cross Sector Cybersecurity Working Group provide a foundation on which we can build. To date, efforts with industry have largely focused on planning. Now is the time for the Department to collaborate with private sector partners to take meaningful steps to share actionable threat, vulnerability and mitigation information with each other and to coordinate research and development activities for new cyber technologies and protective programs.

26. Currently, many distinct components of DHS play a role in the Department's cybersecurity mission including but not limited to: the Office of Cybersecurity and Communications (under the leadership of NPPD), the National Cybersecurity Center, and the Office of Policy. What do you believe are the appropriate roles and responsibilities of the various DHS components with regard to cybersecurity?

I believe the Department is currently organized to deliver expert advice through its components which have responsibility for cybersecurity. Specifically, the Office of Cybersecurity and Communications (CS&C) is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. It has a heavy operational role working with both the federal government and private sector. In addition, CS&C was formed to ensure a proactive Government capability and capacity as the IT and communications sectors continue to converge. CS&C includes the National Communications System (NCS) and National Cybersecurity Division (NCSD) as well as the Office of Emergency Communications, to ensure coordination and synergy between these closely coupled organization.

The National Cybersecurity Center was created to deliver cross-domain situational awareness; analyze and report on the composite state of U.S. cyber networks and systems; and foster collaboration among the six largest federal cyber centers.

Within the Office of Policy, the Director of Cybersecurity Policy Development provides substantive policy guidance related to national cyber risk governance and management. This official helps to develop departmental policy positions and negotiate these positions within the interagency.

There are other components within the Department Headquarters that have a role in Cybersecurity, for example the Office of Science and Technology, the Office of Intelligence and Analysis, as well as other operational components of DHS, including CBP, FEMA and ICE.

27. The Conficker worm has infected millions of computers worldwide. In response to this threat, the federal government and private industry have partnered to share information and develop countermeasures to prevent the spread of the worm and to mitigate its ultimate effect. However, the lines of authority in responding to the Conficker worm are unclear. Consequently, when US-CERT disseminated instructions on how to protect federal systems against the worm, those instructions were ignored by a significant number of agencies.

- a. Do you believe that under the current law there is a clearly designated lead agency for cybersecurity?

No, there is not one clearly designated lead for cybersecurity, and that is because several agencies have different, yet important responsibilities with respect to cybersecurity. DHS' mission, however, places it in prime position to coordinate many of the actions required during situations similar to the Conficker worm. For example, DHS' responsibilities related to the .gov Federal Civilian Executive Branch networks and critical cyber infrastructure positioned it to distribute critical information to Federal and non-Federal partners and mitigate the potential impact Conficker could have had.

- b. In the case of the Conficker worm, what would your response have been if US-CERT had reported to you that a substantial number of federal agencies were ignoring its guidance?

Working with the White House and the Office of Management and Budget (OMB), I would engage with the leadership of those federal agencies to ensure they had complete comprehension of the incident and the potential impact of ignoring US-CERT guidance. As OMB is responsible for the overall implementation of information security activities on Federal Executive Branch networks under the Federal Information Security Management Act (FISMA), it would be a key ally in communicating the importance of an issue such as this to the Departments and Agencies. That said, I would also turn to the Office of Cabinet Affairs and even the White House Chief of Staff if necessary.

28. In addition to the Under Secretary, a number of officials within the NPPD have responsibilities for cybersecurity, including the Deputy Undersecretary of NPPD, the Assistant Secretary of CS&C, and the Director of the United States Computer Emergency Readiness Team (US-CERT).

- a. How will you manage these offices to ensure there is effective leadership and management with regards to cybersecurity?

These roles fall within a clearly delineated chain of command. The Deputy Under Secretary provides not only expertise and senior leadership oversight on cyber issues, but also ensures coordination and collaboration between cyber and physical protection for the Nation's critical infrastructure. It is critical that NPPD's

components are able to effectively coordinate and collaborate. DU/S Reitingger's experience both in government and in industry, as an attorney, a technology leader, and an experienced manager, make him exceptionally qualified for this role.

The Assistant Secretary of CS&C reports to the Office of the Undersecretary of NPPD. CS&C was created, along with an Assistant Secretary position within that Office, in recognition of the importance of cybersecurity and the need for senior appointed leadership focused on this critical topic. The Assistant Secretary is responsible for timely and successful execution of deliverables under the Cybersecurity Initiative to include deployment of the TIC and EINSTEIN 2 and 3 programs, Supply Chain Risk Management, Education and Workforce Development, and improving collaboration with private sector and the security of CIKR networks.

The Director of the US-CERT is responsible for managing DHS' 24x7 cyber operations center. US-CERT analyzes data received from the Einstein sensors, the Intelligence Community, government and industry partners, and other sources to identify threats, vulnerabilities, and trends. US-CERT collaborates with public and private sector partners to develop and promulgate protective and mitigation strategies. US-CERT provides cyber incident response and recovery coordination and support for federal, state, local, tribal and territorial, international and private sector partners. US-CERT also produces products made available to the general public on www.us-cert.gov. The Director of the US-CERT reports to the Assistant Secretary through the Director of the National Cybersecurity Division.

- b. How do you see the responsibilities of the Under Secretary of NPPD in relation to these officials?

The Under Secretary provides overall leadership to all NPPD components and is responsible for setting the strategic direction for the organization. He or she ensures the alignment of the individual components with broader Departmental policies and priorities. The Deputy Under Secretary, the Assistant Secretary of CS&C, and the Director of US-CERT all support the Under Secretary in developing policies and setting Directorate priorities and each is responsible for implementing specific strategies.

29. In January 2008, President Bush signed National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – a multi-agency, multi-year plan that laid out twelve steps to securing the federal government's cyber networks. Also known as the Comprehensive National Cybersecurity Initiative (CNCI), this plan represented a fundamental shift in how the federal government approached cybersecurity and gave DHS new responsibilities as well as a significant increase in funding and staffing to carry out these responsibilities. Specifically, the CNCI gave DHS additional responsibilities for coordinating cybersecurity across all civilian federal agencies. However, the CNCI did not give DHS any authority to compel coordination or compliance across the federal government.

- a. What authorities do you believe DHS needs to effectively secure our federal government networks against ongoing cyber attacks?

Secretary Napolitano is reviewing the response to her Action Directive requesting information on the Department's cybersecurity authorities, responsibilities, programs, and timelines. If confirmed, I look forward to joining her in that review and determining where authorities might need to be strengthened for each of our missions.

- b. What resources do you believe DHS needs to accomplish this mission?

Secretary Napolitano is reviewing the response to her Action Directive requesting information on the Department's cybersecurity authorities, responsibilities, programs, and timelines. If confirmed, I will review and work to determine appropriate resource levels for DHS's various cybersecurity missions.

- c. The CNCI was developed with little input from the private sector even though the private sector owns most of the cyber infrastructure, even in the context of federal information technology networks. What steps will you take to ensure that the private sector is adequately involved in the development of policies and protocols for federal cybersecurity?

It is my understanding that DHS has worked very closely with the private sector to ensure they were represented in the creation of the implementation plans that will be used to meet the DHS-lead initiatives of the CNCI. It is my understanding that the President's 60-day review of cybersecurity engaged the private sector extensively. If confirmed, I look forward to building on the recommendations made through these engagements utilizing the framework outlined in the National Infrastructure Protection Plan in order to ensure all appropriate stakeholders are engaged, our private sector partnership meets our Nation's needs and our Nation's cyber infrastructure is robustly and effectively protected.

30. The CNCI also created the National Cybersecurity Center (NCSC) to synthesize information from various cybersecurity centers across the federal government and develop situation awareness, loosely modeled after NCTC. The NCSC was established in DHS, but outside of the existing structure in the National Cybersecurity Division, with a direct report to the Secretary. Last month, Rod Beckstrom, the Director of the NCSC resigned, stating in his resignation letter that the "NCSC did not receive appropriate support inside DHS during the last administration to fully realize this vital role."

- a. Given that the Director of the NCSC reports directly to the Secretary while the Under Secretary of NPPD reports through the Deputy Secretary for the Department, what is your understanding of how NPPD coordinates its work with NCSC or responds to requests from NCSC?

NCSC and NPPD are but two DHS components with responsibilities regarding cybersecurity – other components such as S&T, Policy, and the United States Secret

Service also play key roles. We must coordinate among all these components, and also with departments and agencies outside DHS to be fully effective, and that will be a key role both for me, if confirmed, and for DU/S Reitingner. In particular, US-CERT must rapidly respond to and fully participate in NCSC actions as one of its key stakeholders.

- b. Do you believe any organizational changes are necessary within DHS regarding the relationship between the NCSC and NPPD?

The Department is exploring options to more effectively align the operations of NCSC and the work of NPPD while remaining faithful to the interagency mission of NCSC. We hope to move forward in the near-term.

Chemical Site Security

31. Congress authorized the Department's chemical site security program, now known as the Chemical Facility Anti-Terrorism Standards (CFATS), as part of the Department of Homeland Security Appropriations Act, 2007 (P.L. 109-295). While the original authorization for the program expires this year, it appears that both Congress and Secretary Napolitano are committed to keeping the program going. If confirmed as Under Secretary for NPPD, you would be responsible for overseeing the CFATS program and would presumably play a significant role in efforts to reauthorize the program.

- a. What is your assessment of the CFATS program to date?

Based on my current knowledge of the CFATS program, I believe that it is an effective program for addressing the security risks associated with the Nation's high-risk chemical facilities and is helping to make the country more secure. Implementation is now underway and CFATS is working to improve security at high-risk facilities, and will even more significantly enhance security and protect communities as the program matures.

In the two and one-half years since the Department was granted authority to regulate security at high-risk chemical facilities, I believe the Department has developed an effective approach for both identifying high-risk chemical facilities and assessing the security risks associated with them. To date, the Department has reviewed consequence assessments (Top-screens) for more than 36,000 potentially high-risk chemical facilities, from which the Department has preliminarily identified approximately 6,400 facilities as preliminarily high-risk. Of those preliminarily high-risk facilities, over 5,600 have submitted Security Vulnerability Assessments (SVA). It is my understanding that the Department is in the process of reviewing those SVAs, and will very soon issue the first set of final tiering determination letters to approximately 140 Tier 1 facilities, and set the due date for their Site Security Plans (SSP). The Department will simultaneously release the next module of the CFATS online suite of compliance tools, the SSP template and instructions, as well as the

Risk-Based Performance Standards Guidance Document, which will assist facilities in completing the SSPs.

- b. Do you believe the CFATS program needs any significant modifications and what impact do you believe any such programmatic changes would have on the existing program?

I believe that CFATS needs to be made a permanent program. Currently, CFATS is slated to expire in October 2009 if not reauthorized by Congress. I would urge the Congress to act to ensure continued implementation of this important program without requiring extensive revisiting of the program currently in place. As previously stated, I believe that CFATS is enhancing security by helping to ensure high-risk chemical facilities throughout the country have security postures commensurate to their level of risk.

- c. Do you believe the CFATS program should be expanded to include drinking water and wastewater facilities?

I believe that there is an important gap in the framework for regulating the security of chemicals in the United States, in that the current statutory authority for CFATS excludes from its coverage water and wastewater treatment facilities. I think that the Department needs to work with the Congress to close this gap in authorities in order to secure chemicals of concern at these facilities and protect the communities they serve. Water and wastewater treatment facilities that are determined to be high-risk due to the presence of chemicals of concern should be regulated for security in a manner that is consistent with the CFATS risk and performance-based framework.

- d. Do you believe the CFATS program should be harmonized with the MTSA chemical facility security regulations? If so, how?

Because CFATS and MTSA both address chemical facility security, there certainly should be harmonization, where applicable, between these programs. I am aware of this issue and if confirmed, will ensure it is fully explored and appropriately addressed. I think it's important, for example, to have full visibility on what chemicals of interest are out there, whether at facilities subject to MTSA or facilities potentially subject to CFATS, so that security risks can be evaluated at the national level.

- e. What role do you expect your office to play regarding a reauthorization effort and what, if any, challenges do you foresee in this effort?

As the entity responsible for implementing CFATS, I believe NPPD and IP are in an excellent position to provide insight on the experience and lessons learned during the first years of developing and implementing CFATS. We welcome the opportunity to continue to engage with Congress as permanent CFATS legislation is developed, and to assist in any way that Congress believes would be helpful.

32. In 2006, you co-chaired a task force on homeland security established by the Century Foundation, which issued a report titled "The Forgotten Homeland." That report, which predated the establishment of the CFATS program, included a chapter on chemical site security that called for a rigorous regulatory program to be established at DHS. Some elements of the CFATS program – such as the use of tiering and performance standards – track recommendations from the report. However, the CFATS program does not incorporate other elements that were recommended by the report.

- a. Do your views on chemical site security generally track those expressed in the report? If not, please discuss any differences you may have with the recommendations.

Yes.

- b. The report says an effective chemical site security program should be sufficiently rigorous to give high risk facilities an incentive to implement safer technologies or move dangerous operations to more remote locations as a means to achieve greater security. Do you agree with this view? Do you believe the CFATS program as currently designed provides meaningful incentives for facilities to adopt safer technologies as a means of increasing site security?

Based on my understanding, CFATS currently provides facilities with flexibility to assess and determine how they will meet the Risk-Based Performance Standards applicable to their tier. This could include adoption of safer technologies where appropriate. CFATS also allows facilities to notify the Department by submitting a revised Top Screen when they make a material modification, such as changing holdings of a CFATS chemical of interest. I understand that some facilities that have voluntarily made changes to, among other things, their chemical holdings and distribution practices, and that NPPD supports such measures to reduce risk, as long as they do not shift risks inappropriately.

- c. Do you believe the CFATS program's current requirements for the physical protection of a facility are sufficient?

Yes, the Risk-Based Performance Standards (RBPS) address specific areas related to physical protection, and a final high-risk facility will articulate in its SSP how it will meet each applicable RPBS with security measures appropriate for its tier level and facility-specific circumstances. The RBPS are:

1. Restrict area perimeter
2. Secure site assets
3. Screen and control access
4. Deter, detect, delay
5. Shipping, receipt, and storage
6. Theft and diversion
7. Sabotage

8. Cyber
9. Response
10. Monitoring
11. Training
12. Personnel surety
13. Elevated threats
14. Specific threats, vulnerabilities, or risks
15. Reporting of significant security incidents
16. Significant security incidents and suspicious activities
17. Officials and organization
18. Records

- d. The same report recommends providing liability protection and terrorism insurance premium reductions for chemical facilities that are in compliance with a federal security program such as CFATS. Do you agree that recommendation?

I certainly think that we should look into it.

33. The authorizing language and subsequent regulations for the CFATS program generally shields data about the program, including site vulnerability assessments and security plans, from public disclosure, although it does allow for some information sharing with certain state and local government officials possessing the necessary security clearances. This information is given a new designation – Chemical Vulnerability Information or CVI – and is subject to strict controls.

- a. Do you think the CVI provisions strike the correct balance between protecting sensitive information and allowing for adequate accountability for the CFATS program?

Based on my current understanding of the program, I believe that Chemical-terrorism Vulnerability Information (CVI) successfully strikes a balance between protecting sensitive information companies have provided to the government under CFATS and ensuring appropriate information-sharing with our security partners at the Federal, state, and local level, as well as ensuring adequate accountability for the CFATS program. CVI was specifically designed to address information sharing and protection concerns surrounding chemical facilities potentially regulated under CFATS. Individuals in possession of CVI must verify that the individual with whom the CVI will be shared is both: (1) a CVI Authorized User (i.e. successfully completed CVI training and been issued a CVI Authorized User number by DHS) and, (2) has a “need to know” that specific CVI.

- b. How should the CVI program relate to the broader effort to create a more unified framework for all controlled unclassified information to allow for more effective information sharing?

I understand that the Department supports the government-wide effort to create a more unified framework for all controlled unclassified information and is committed to its successful implementation. I also understand that the Department seeks to align CVI, to the degree possible, with direction and guidance relating to the implementation and execution of controlled unclassified information. The provisions of the CVI program as they relate to need to know, authorized users and handling protocols are important to the ability to assure chemical facility owners and operators that their information will be protected, and continuing the ability to share information with other Federal, State and local authorized users with need to know.

Intergovernmental Affairs

34. The Homeland Security Act established the Office for State and Local Government Coordination – a forerunner of the current Office of Intergovernmental Programs – in the Office of the Secretary. In a subsequent reorganization undertaken by the Department under section 872 of the Homeland Security Act, this Office was moved into the then-existing Preparedness Directorate. Under the Post-Katrina Emergency Management Reform Act, the Office – along with much of the rest of the Preparedness Directorate – was statutorily merged with FEMA. Currently, the Department through budget and appropriations mechanisms manages the Office as part of NPPD.

- a. Do you believe that the use of these mechanisms is consistent with the merger required by the Post-Katrina Act?

I have been briefed on the history of the Office of Intergovernmental Programs, and the past movement of the Office. These actions were undertaken during the previous Administration. It is my understanding that the FY 2010 President's budget request seeks to move the Office of Intergovernmental Programs from FEMA to the Office of the Secretary. The Assistant Secretary of IGP would then report directly to the Secretary. I believe that the Secretary of Homeland Security should have a dedicated office to liaise with State, local, tribal and territorial governments.

- b. Do you believe the Office of Intergovernmental Programs should be part of NPPD? If so, how do you see it fitting into the overall mission of NPPD and what steps would you take to improve it?

As noted in my previous response, I believe that the Office should be a direct report to the Secretary of Homeland Security as requested in the President's FY 2010 budget submission.

Office of Risk Management and Analysis Questions

35. There has been substantial debate in the last several years as to how to conceptualize, quantify, and manage homeland security-related risk.

- a. How do you personally assess the issue of homeland security-related risk?

Homeland Security risks arise from potential acts of terrorism, natural disasters, and other emergencies and threats to our people and economy, as well as violations of the Nation's borders that threaten the lawful flow of trade, travel, and immigration. I assess, as does DHS, homeland security risk by evaluating the potential for an unwanted outcome as a function of threats, vulnerabilities, and consequences associated with all hazards to the homeland.

- b. Which experiences from your career inform your perspective on risk? How should the various components of risk (e.g. threat, vulnerability, consequence) be assessed and weighed?

My entire career, including my time at the NSC, has informed my perspective on risk. The assessment and weighting of risk variables (including threat, vulnerability, and consequence) is dependant on a variety of considerations, including availability of information, the decision context, and resource (staffing, time, etc.) constraints. Threat, vulnerability, and consequence can each be addressed in many ways, but they need to be addressed in a comparable manner. In addition, any risk analysis methodology needs to be tested, reviewed, validated, and have a built-in lessons learned process to ensure that it is defensible, that it benefits from outside perspectives, and that it has a process for continuous improvement.

- c. How should risk and risk assessment be used to inform the Department's activities and priorities?

Understanding and managing the risks to the American homeland is a fundamental task of homeland security. Since its inception, DHS and its partners have espoused the principle that homeland security decisions should be risk-informed. This principle has been articulated and repeated in a multitude of high-level policy documents, including presidential directives, national strategies and plans, and Department-level strategic and policy documents. Components and programs within the Department have taken this requirement seriously and worked to build the ability to fulfill it.

Managing homeland security risk depends on making prioritization tradeoffs across the entire homeland security mission space. These tradeoffs need to be made among disparate programs, which are designed to address a variety of risks including terrorism, natural disasters, immigration and customs issues, among others. Doing this requires identifying the risks to homeland security; assessing those risks in a comparable manner, transparently, and defensibly; determining alternative courses of action to manage those risks; making and implementing decisions amongst those alternatives; and monitoring and evaluating the actions taken to ensure they are performing as expected and reducing the risks to the Nation.

36. Do you agree that risk management should consider a wide variety of costs, including costs to regulated private sector entities and a policy's impact on privacy and civil liberties

Yes, the costs to regulated private sector entities, policies that impact on privacy, as well as many other costs should be considered.

37. The DHS Office of Risk Management and Analysis (RMA) was established within NPPD in 2007, and is intended to "lead the Department's efforts to establish a common framework to address the overall management and analysis of homeland security risk." The Under Secretary for NPPD chairs the Department-wide Risk Steering Committee.

- a. Based on your work on the DHS Agency Review Team and your work at the Department to date, what is your assessment as to how effective the RMA office has been in its first two years of existence?

I think that RMA has been effective. I have been briefed on RMA's efforts and I understand that the office has created the Department-wide Risk Steering Committee (RSC), to serve as the Department's risk management governance structure; published the DHS Risk Lexicon through the RSC; completed the first prototype for the Risk Assessment Process for Informed Decision-making (RAPID), to inform strategic policy and budgetary decision making by taking into account risk, risk reduction efforts, and alternative resource allocation strategies; published a set of Analytical Guidelines for DHS and its components to improve their risk management capabilities; supported HSPD-8 Annex 1 by drafting the risk management annex (Annex D), which was published as part of the Integrated Planning System; and led the development of the Department's Interim Integrated Risk Management Framework published in January 2009. The Framework provides a foundation for developing subsequent policy, doctrine and guidance that will institutionalize integrated risk management in the Department. That said, the concept of risk-based decision making is an evolutionary process, and more development is needed.

- b. Do you believe the office should continue to exist in its current form in NPPD? If so, what are your plans to improve the effectiveness of this office and its integration of activities across the Department? If not, how would you recommend risk assessment issues be addressed across the Department?

Yes, I believe that RMA should remain as a component of NPPD. RMA is a core NPPD function at the heart of DHS's efforts to match requirements and resources in a prioritized manner to ensure that we focus on the protection and resiliency of our most critical infrastructure and key resources.

I plan to continue to support RMA as it works collaboratively across DHS and in conjunction with its homeland security partners to build an integrated risk management program that ensures that risk information and analysis are provided to decision-makers to inform a full range of decisions. These decisions include the allocation of resources, provision of preparedness assistance, prioritization of capability development, operational decisions, regulatory actions undertaken, and

research and development investment. This integrated risk management program should be based on the establishment of:

- An integrated framework;
- An assessment of the risks facing the Nation and its security domains, as well as the risks to DHS missions;
- Processes to determine possible risk management strategies, and analyze alternative courses of action and homeland security countermeasures, in terms of costs, risk reduction benefits, and likely effectiveness; and
- Metrics to evaluate how effective activities are at reducing risks.

38. GAO has kept “Implementing and Transforming the Department of Homeland Security” on its High-Risk List from 2003 to the present. The Department’s 2008 Corrective Action Plan for removing this issue from the High-Risk List¹ discussed the Department’s development of a strategic risk management framework within the context of broader management processes, including the establishment of a DHS Risk Steering Committee and the Risk Analysis Process for Informed Decision-Making (RAPID), which is intended to serve as a Department-wide process that integrates risk into strategic planning, programming, budgeting, and execution processes.

- a. Do you intend to continue implementing the risk management section of the GAO Corrective Action Plan? What modifications, if any, would you recommend be made to this section of the plan?

The Under Secretary for Management has designed and implemented a management framework based upon the need to address various Department challenges. This framework is the foundation for the Department’s transformation and outlines the manner by which strategic goals are developed, resources are utilized, and performance is monitored and is enabling DHS to manage and overcome all GAO high risk challenges. Part of this framework is the Risk Assessment Process for Informed Decision-Making (RAPID), which is led by RMA.

RAPID’s goal is to provide a common and consistent approach for top-level decision-makers to assess programs across the Components in a single framework. RAPID supports strategic policy and budgetary decision making by assessing risk, evaluating risk reduction effects of DHS programs, and evaluating alternative resource allocation strategies. Once requirements are developed by the Strategic Requirements Planning Process, RAPID will help prioritize various strategic requirements aimed at different goals and objectives.

NPPD will continue to support Management and make adjustments as required to ensure effective execution of the Corrective Action Plan.

¹ http://www.whitehouse.gov/omb/expectmore/issue_summary/issueDetailedPlan_22.pdf

- b. How is RAPID being integrated into the strategic planning, programming, budgeting and execution processes of the Department? Please provide several recent examples.

The Secretary of Homeland Security has committed to using risk analysis to inform resource allocation through the Department's Planning, Programming, Budgeting and Execution (PPBE) process. RAPID currently is the Department's primary assessment tool for providing risk information to the planning, programming and budgeting phases of the process. Although RAPID is currently in prototype, it is already being integrated into the process. Specifically,

- The FY 2011-2015 Integrated Planning Guidance (IPG) defines RAPID's application and mandates participation amongst the DHS components in the annual process to support the build of the FY 2012-2016 IPG.
- The IPG states that RAPID will produce usable results related to chemical and biological terrorism scenarios and DHS' efforts to manage the risk of those scenarios for the purpose of informing decisions.
- The FY 2011-2015 Resource Allocation Planning (RAP) process requires components to link their program budget request to risk reduction areas so as to be used to gather information and support RAPID analysis.
- RAPID's early efforts to map DHS operational programs to risk reduction areas have enabled the Department to better identify gaps in seams in its risk management efforts and has supported work done by the Program Analysis and Evaluation (PA&E) office within the Management Directorate to develop an integrated budget.
- The creation of the RAPID working group, co-chaired by RMA, the Office of Policy, and PA&E, has created a forum for which planners, risk analysts, and budgeters from across the Department convene to evaluate potential methods for enhancing component-level risk-informed decision-making in support of RAPID and building Department-wide processes.
- In the future, RAPID results will be used, as appropriate, to more fully inform both the development of the IPG – which articulates annual priorities for the Department, enable the creation of program risk reduction metrics, and support resource tradeoff decisions across disparate programs. The second prototype of RAPID will be an opportunity to test these applications and more fully integrate RAPID into PPBE.

39. A March 2008 presentation by the Deputy Director of the RMA office (formerly available at <http://risk.lanl.gov>) indicated that one of the objectives of the office was to "Develop the Department's Risk Communication Strategy."

- a. Is this still an objective of the RMA office? If so, what are the plans and timeline for the development of such a strategy?

Among RMA's objectives is improving the Department's risk communications efforts. RMA supports the development of the Department's risk communications strategy through its work to develop a Department-wide integrated risk management capability to

enhance DHS' ability to identify, analyze, assess and communicate risk to support decisions about strategies for managing that risk. Part of the effort is to ensure that the Department has processes in place to share information with key stakeholders and communicate with the public about homeland security risks and efforts being taken to manage those risks. Such communications depends on the ability to build two-way communications mechanisms and establish DHS as a trusted provider of information related to homeland security risks.

- b. What is your personal assessment of the Department's risk communication efforts since its establishment in 2003?

While DHS has made some achievements, more remains to be done within DHS and externally.

A good indication of the importance of risk communications is the Department's experience in the past weeks. As the outbreak of the H1N1 flu virus and the response by DHS and its partners indicates, DHS has made great strides in its risk communications efforts. The Office of Infrastructure Protection was conducting conference calls with CIKR public and private sector partners and the Secretary, in her role as the principal federal official, was able to coordinate across the Federal government to ensure that accurate information was provided to the public to support the ability of individuals and groups to take proactive and appropriate action.

Having said that, there is still work that needs to be done to improve the Department's risk communications efforts, however. RMA working on behalf of DHS will continue to work to advance DHS risk communications efforts.

- c. Do you support increased transparency in the Department's assessment of risk? Should the Department publish a concise list of its assessment of the top threats and vulnerabilities that the nation faces?

I support the idea of transparency in the Department's programs, including our work related to identifying threats to our Nation's critical infrastructure and key resources. I support sharing threat assessment information with both the private sector as well as the public as a whole. However, I believe that vulnerability information should not be publicly disseminated.

As an example, in 2007, the inaugural Homeland Security Threat Assessment (HSTA) was published as an assessment of the major threats to the Homeland for which the U.S. Government must prepare and respond—to include the actions, capabilities, and intentions of domestic and foreign terrorists and extremists and the possible occurrence of systemic threats. The HSTA was not classified and was released to our private sector partners through formal information sharing channels

including the Homeland Security Information Network (HSIN). The HSTA was a good step forward even though much more needs to be done. For example, the HSTA did not address natural disasters or the full scope of threats that fall within the statutory responsibilities of the individual Components of DHS.

40. The 9/11 Commission Recommendations Act includes amendments to the Homeland Security Act governing the distribution of grants under two of the major homeland security grant programs, the State Homeland Security Grant Program (SHSGP) and the Urban Area Security Initiative (UASI). These provisions guarantee each state a minimum allocation under SHSGP, but otherwise largely leave to the Secretary's discretion the allocation of grant funds to states and high-risk urban areas based on a jurisdiction's relative threat, vulnerability and consequences faced from acts of terrorism and on the anticipated effectiveness of the proposed use of the grant, provided that certain basic risk factors are taken into account.

To help it allocate grants, DHS has developed (or contracted with others to develop) a terrorism risk model. Reflecting the difficulties in determining the true risk of terrorism, however, the model in past years has been incomplete, depended on subjective weighting and has been difficult if not impossible to externally validate. Given the uncertainties inherent in measuring the risk of terrorism, how would you approach the issue of risk analysis for the purposes of distributing homeland security grants and what criteria would you use to evaluate whether a proposed method for allocating grants is appropriate and adequately reflects the likely risk of terrorism? Do you believe that DHS's current risk model should be changed?

The major homeland security grant programs are administered within DHS by the Federal Emergency Management Agency (FEMA) and the risk model to determine allocation eligibility has been developed by FEMA in conjunction with the risk community across DHS. The risk formulas used in the SHSP, UASI, Transit Security Grant Program (TSGP), Port Security Grant Program (PSGP) and Interoperable Emergency Communications Grant Program (IEGCP) are all based on a common formula. Each of the formulas have different variables, however, depending on the grant program. For example, the Transit Security Grant Program measures ridership on transit systems, but the Port Security Grant Program looks at variables such as domestic cargo volume. The basic form is derived from standard risk theory: namely, risk is the *Likelihood* of an adverse event occurring multiplied by the expected value of the *Consequence* were that event to occur.

RMA is working with FEMA's Grants Program Directorate to support its efforts to refine and improve the existing methodology for the Interoperable Emergency Communications Grant Program for the FY 2010 cycle, in order to more accurately capture the multi-hazards risk. The Interoperable Emergency Communications Grant Program is jointly administered by FEMA and the Office of Emergency Communications in NPPD. The work will seek to bring an evaluation of both the risk of terrorism and selected natural disasters into the grant formula to determine State eligibility amounts for the IECGP.

In response to the specific question of the existing terrorism risk model, it is important to note that we will never know the “true” (i.e., objectively measured) risk of terrorism. Risk is a concept that is inherently related to uncertainty, and terrorism risk includes additional factors of uncertainty such as the threat from an adaptive adversary and the ability for mitigation measures to deter, shift, or reduce risk. Further, the assessment of terrorism risks will always be dependant on subject matter expert opinion, as historical data cannot be relied upon. It would be a mistake to establish the expectation that a terrorism risk formula could ever produce a “true” view of risk. The criteria for evaluating a risk analysis, such as the grant allocation, should be 1) is it useful in the decision being made; 2) is it methodologically defensible; 3) does it utilize appropriate information in an analytically sound manner; and 4) are the results appropriately transparent and communicated in a usable manner.

41. The RAND Corporation noted in a 2004 report, “When Terrorism Hits Home: How Prepared are State and Local Law Enforcement,” that “[h]omeland-security experts and first-responders have cautioned against an overemphasis on improving the preparedness of large cities to the exclusion of smaller communities or rural areas, noting that much of our critical infrastructure and some potential high value targets (nuclear power plants, military installations, agriculture facilities, etc.) are located in less-populated areas.” Moreover, we know that al Qaeda attackers lived, trained, transited, hid, and otherwise used smaller communities and rural areas as a staging ground for the September 11, 2001 attacks. Do you agree that smaller communities and rural states and localities need to receive adequate federal assistance to prevent, prepare for, respond to, and recover from terrorist attacks?

The Secretary has noted publicly that risk exists everywhere in both urban and rural areas. As such, I support an approach to grants that address all the threats and risks faced by communities whether natural or man-made.

US- VISIT

42. The previous Administration, in placing US-VISIT within NPPD, argued that US-VISIT was not just a border management program, but that it interacted with a number of different federal agencies and thus fell within the overarching theme of the NPPD. Part of the rationale for this was an argument that US-VISIT was not a terrorism prevention program as much as it was an identity management/immigration program.
 - a. What is your assessment of this contention?

US-VISIT primarily provides biometric based, identity verification services—the collection, storage, matching, and analysis of biometric-based data—to the immigration and border management, law enforcement, and intelligence communities. While US- VISIT continues to fulfill its original mission of implementing an integrated entry and exit system for the United States, US-VISIT

has evolved into a Department-wide resource for biometric storage and matching. I believe that it is for this reason that US-VISIT is not associated with a single operational DHS component. Instead, it is organizationally situated to provide services to the entire Department as well as other Federal agencies. Additionally, the management of the contained data and the acquisition of new data require Department-led attention.

- b. Please provide specific examples of how the US-VISIT program coordinates or shares information with non-DHS law enforcement entities.

The Departments of Justice, State, and Homeland Security signed a memorandum of understanding that creates an agreed-upon framework for the three departments to share their biometric data. DHS and the Federal Bureau of Investigation (FBI) are working to establish full interoperability between the DHS/US-VISIT Automated Biometric Identification System (IDENT) and the Integrated Automated Fingerprint Identification System (IAFIS) of the FBI's Criminal Justice Information Services (CJIS) Division. Through this interoperability, US-VISIT is able to provide DHS biometric data to State and local law enforcement agencies, through CJIS, which enables the identification of non-citizens who are of an interest to the U.S. Immigration and Customs Enforcement (ICE). This sharing of biometric information also enables the DOS to better screen visa applicants against not only DHS data but also FBI criminal history. Additionally this interoperability allows the US Office of Personnel Management (OPM) to run federal job applicants against the DHS database to identify those individuals who are not US citizens and ineligible for federal employment. Furthermore, this interoperability allows DOD to run fingerprints collected during overseas operations against the DHS data which results in them being able to identify those individuals that have visited or attempted to visit the United States.

In addition US-VISIT has provided DHS biographic arrival and departure information that has enabled DOS to identify fraudulent visa application activities. Currently DHS and DOS are working to establish a real time system to system interface which will enable all consular officers to have access to DHS arrival and departure data.

- c. What specific actions will you take if confirmed to ensure that US-VISIT is proactively engaging the general law enforcement community to ensure that its services are used by other agencies and departments?

A prime example is US-VISIT's support of the Department's mission through the US-VISIT Executive Stakeholder Board (ESB), a formal structure that US-VISIT uses to coordinate with other agency stakeholders. The ESB is a forum in which US-VISIT can solicit input from, and discuss issues with, the customer agencies it supports. The ESB has enabled US-VISIT to coordinate its budgets to ensure that the operational missions of its customer agencies are met. For purposes of the ESB, stakeholders represent a DHS component or office. The members of the ESB include DHS components CBP, ICE, CIS, USCG, TSA, FEMA, and the Secret Service. If

confirmed, I will support US-VISIT's mission by ensuring that the ESB includes representation from non DHS entities such as DOD, DOJ and DOS to ensure that all mission requirements are being coordinated and considered.

- d. Do you believe the US-VISIT program is an immigration program or a terrorism prevention program? Is such a distinction valid?

The US-VISIT program is a biometric identity service provider that supports decisionmakers implementing the DHS mission. That mission includes border security, immigration management, antiterrorism, disaster response and recovery, and infrastructure protection, among other goals.

US-VISIT was created as a critical component of the DHS strategy to protect our Nation from dangerous people and to facilitate the movement of legitimate travel and trade—a role it continues to fulfill today. However, US-VISIT's value is not limited to border security and immigration management. US-VISIT provides the capability for DHS components and other agencies to establish an individual's identity through the capture of biometric information and its association with biographic information. Decisionmakers are able to access information, appropriate to their business needs, associated with any one individual, including the results of watchlist and criminal background checks.

43. In 2008, GAO raised concerns that US-VISIT, despite making progress towards identifying and implementing strategic goals, had “yet to fully define its relationships with other immigration and border management programs.” GAO was particularly concerned about the lack of a cohesive strategy for integrating other Customs and Border Protection (CBP)-run border management programs such as SBInet and the Western Hemisphere Travel Initiative with the US-VISIT program.

- a. Given that the US-VISIT program is administered by CBP in the field, why does its placement in NPPD make sense?

While CBP is a major contributor to the US-VISIT biometric data base, US-VISIT provides a Department-wide service in biometric storage and matching. In addition, US-VISIT provides services to ICE for interior immigration enforcement; to the U.S. Coast Guard for interdiction operations; to the Transportation Security Administration (TSA) for vetting and credentialing of airport workers; to U.S. Citizenship and Immigration Services (USCIS) for immigration benefits; to the Department of State for visa applications; and to the FBI for law enforcement purposes. The placement of US-VISIT in NPPD recognizes that US-VISIT has evolved from a border control program created to address specific legislative mandates to an organization that is a strategically placed for the entire Department.

- b. What specific actions will you take if confirmed to ensure that US-VISIT is proactively coordinating with CBP to ensure that its technology and program goals

are integrated into other border management programs?

US-VISIT is actively engaged with CBP to complement its border management programs and meets regularly with CBP's Offices of Field Operations, Border Patrol, Air and Marine, and Information and Technology. Additionally, CBP has detailed CBP officers to US-VISIT. As an example, US-VISIT is working with CBP, the DHS Office of Policy, and USCIS on a pilot project to test the collection of biometrics from the holders of H-2 visas for temporary and seasonal workers who exit the United States. The pilot will be conducted at two locations: the Douglas and San Luis, Arizona, ports of entry. It specifically addresses the requirement to expand exit so that persons who overstay limited-duration visits to the United States can be identified.

44. In December of 2008, GAO issued a report that criticized US-VISIT for failing to "fully satisfy any of the eleven conditions required of DHS by the Consolidated Appropriations Act of 2008, either because the plan does not address key aspects of the condition or because what it does address is not adequately supported or is otherwise not reflective of known program weaknesses." In particular, GAO reported that US-VISIT had failed to adequately implement its risk assessment model, that the program's air-exit solution used cost estimates that were not realistic, and that its expenditure plan had not met congressional conditions. This was the latest in a long line of GAO reports criticizing the agency for failing to meet congressional requirements.

- a. If confirmed, what specific actions will you take to ensure that US-VISIT complies with legislative mandates?

If confirmed, I will review the report and consult with the Committee on a way forward.

- b. What specific actions will you take to address GAO's concerns about the failure to adequately and proactively implement the risk assessment model?

If confirmed, I will review the report and consult with the Committee on a way forward.

- c. What specific actions will you take to ensure that cost estimates associated with US-VISIT programs are realistic?

US-VISIT has taken numerous steps to improve its cost estimating practices. They include:

- Hiring experienced and certified cost estimating personnel to improve development of both project estimates and the program life cycle cost model.

- Program participation in the development of the new GAO Cost Assessment Guide, GAO's best practices manual for cost estimation, over the last year.
- Involvement of the Cost Analysis Division, Office of the DHS Chief Procurement Officer, in the review and improvement of program estimates and estimating practices and techniques.
- Active engagement in the adoption of recently developed DHS program acquisition management policies and procedures (e.g., Acquisition Directive 102-01) that will facilitate the improvement of program cost estimates.

Additionally, US-VISIT has worked with GAO to provide a detailed program cost analysis self-assessment, with corresponding documentation, to remove the outstanding recommendation to improve program cost estimation. Follow-up discussions with GAO are scheduled in the next 10 days and initial responses indicate closure of this recommendation is imminent.

45. A biometric entry and exit program is considered by many people, including the 9/11 Commission, to be a vital component of homeland security. DHS has failed to meet a number of statutory deadlines associated with the exit component of the US-VISIT system, and is currently working on a pilot program for the airport exit component that was required by the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act of 2009 (P.L. 110-329). In its announced notice of rule making, DHS proposed that the air carriers be responsible for collecting biometric exit data from eligible travelers and allowing the carriers to decide where in the airport this collection would take place. The airlines have complained that this represents an unfunded mandate and that they are being asked to take on a federal responsibility.
- a. Do you believe that a biometric exit system is needed? Please explain your reasoning either for or against a biometric exit system.

US-VISIT's efforts to plan, develop, and deploy biometric exit capabilities are directly aligned with the Department's core mission and goals. The use of biometric and biographic data gives officials the information needed to authenticate travel documents; verify identity; and identify criminals, immigration violators, and other individuals who may threaten the Nation's security. Moreover, there are considerable law enforcement and intelligence benefits from being able to accurately document the entry and exit of foreign nationals and to conduct trend analyses on arrivals and departures. Additionally, accurately identifying individuals who stay in the United States beyond their authorized periods of admission (overstays) allows DHS to focus resources on addressing known (confirmed) overstays and permit both DHS and the Department of State to place greater emphasis on properly adjudicating travel and immigration benefits. The data collected on overstays supports the Visa Waiver Program in providing information to assist in determining what countries should be considered for inclusion of the Visa Waiver Program.

b. What should be the goal of an exit system?

I believe that the goal of an exit system is to assist in the enforcement the Nation's immigration laws. It requires the capability to determine whether foreign nationals have legally entered and exited our country and complied with the terms of their admission. Decision-makers must determine who is in the United States, who is eligible to enter the United States, and who may have violated the terms of their admission or benefits. A comprehensive biometric exit recording and processing capability will significantly improve US-VISIT's ability to completely and accurately match entries and exits and to identify overstay. It will also provide another opportunity to identify individuals who, upon subsequent analysis, are determined to be criminals, potential terrorists, or other persons of interest.

c. If confirmed, what steps would you recommend DHS take to ensure that an exit component is deployed to the airports as soon as possible?

I believe that DHS and US-VISIT are already taking the steps necessary to deploy Air/Sea Biometric Exit as expeditiously as possible, such as by publishing a notice of proposed rulemaking, conducting the upcoming pilots in two locations, and evaluating the pilots to determine the path forward for Air/Sea Exit. I would support US-VISIT in its continued efforts.

d. Do you believe that the airlines should be responsible for collecting biometric exit data for the US-VISIT program? If not, who do you think should be responsible for this data collection?

Due to the limited existing infrastructure and processes for air and sea exit inspections, DHS considered all possible options for implementing Air/Sea Biometric Exit. Per the direction of Congress, DHS will not decide responsibility or location for implementing Air/Sea Biometric Exit until further information is available from the planned air exit pilots. These decisions will be articulated in the final rule for Air/Sea Biometric Exit. I will reserve judgment on this matter until DHS has the opportunity to review the results of the pilot program.

46. Some have argued that the only logical place for the collection of exit biometric data is at the gate as people are entering the jetway, to ensure that individuals cannot enroll their biometrics in the system and then leave the airport – something that would be possible if the data were collected at any other location in the airport.

a. What is your assessment of this argument?

As mentioned above, DHS will be conducting two Air Exit pilots very shortly. One of the pilots will involve CBP officers taking biometrics at the gate. The results of this specific pilot, combined with results of the pilot involving TSA at the security

checkpoint, will help the Department, and myself reach a fully informed decision on the best way to implement a biometric Air Exit solution.

b. Where do you believe that the exit data collection should take place?

DHS will not decide the responsibility or location for implementing Air/Sea Biometric Exit until further information is available from the planned air exit pilots. The pilots will test two of the options as proposed in the notice of proposed rulemaking published last year. After the evaluation of the pilots, DHS will articulate a decision in the Final Air/Sea Biometric Exit Rule.

c. What is the law-enforcement benefit to ensuring that individuals cannot exit once their biometric information has been collected by US-VISIT?

The benefit to ensuring that individuals cannot exit until their biometric information has been collected is that immigration law enforcement will have a better sense of who has left and who has not, and will be able to allocate resources to apprehend illegal overstays. A clear picture of who has left is necessary to ensure that U.S. Immigration and Customs Enforcement does not deploy enforcement resources in pursuit of individuals who have already departed the country but whose exit was not recorded.

47. Collection of biometric exit data at the land border is highly problematic due to the current lack of outbound infrastructure at the Ports of Entry (POE) and the fact that the U.S. does not currently require exit inspections of all travelers.

a. Do you believe that the collection of biometric exit data should also take place at the land POEs?

Implementing the biometric confirmation of the departure of travelers via land ports of entry is significantly more complicated and costly than for air or sea environments. Enabling biometric, much less biographic, collection of data upon exit would require a massive expansion of exit capacity, including physical infrastructure, land acquisition, and staffing. That said, it is my understanding that US-VISIT believes it is possible to develop and deploy a biometric exit capability at U.S. land borders. US-VISIT continues to pursue a deliberate, phased, and tailored approach to implementing a biometric land exit recording system over the next several years.

b. What steps would you take to ensure that DHS continues to examine the issue of exit data collection at the land border?

I will work with Department leadership so that, as land exit policy is formulated, the process is informed by the subject matter expertise of US-VISIT. I believe that the implementation of Air/Sea Biometric Exit is DHS's priority.

- c. Do you believe that the current focus on southbound smuggling of guns and cash into Mexico by the cartels, which has led DHS to increase its southbound inspections, may provide an opportunity to reassess the feasibility of enhancing southbound infrastructure and implementing southbound inspections on a more systemic basis? What would US-VISIT's role and function be in such a decision making process?

The inspection of outbound vehicles is a CBP operation. Should DHS decide to do so, US-VISIT would support CBP operations in the identification of foreign nationals who are stopped, as well as vetting those individuals against watchlists.

- d. The President's budget overview includes \$45 million for an exit pilot at key land ports of entry. What is your understanding of the details of this exit pilot?

The budget funds \$45 million for the expansion of an exit pilot at key land ports of entry and other border security priorities. A portion of this \$45 million will be used by DHS for departure recording activities.

Specifically, on August 10, 2007, former DHS Secretary Chertoff and former Commerce Secretary Gutierrez announced a 26-point immigration plan that the Bush Administration would pursue to address border security and immigration challenges. One of these initiatives included the establishment of a new land border exit system for guest workers, starting on a pilot basis. This will help ensure that temporary workers in the United States now follow the mandate to leave when their work authorization expires.

On February 13, 2008, DHS published a notice of proposed rulemaking (NPRM) proposing changes to requirements affecting temporary and seasonal agricultural workers within the H-2A nonimmigrant classification. On August 20, 2008, DHS published an NPRM proposing changes to requirements affecting H-2B nonimmigrants H-2B (temporary nonagricultural workers) and their employers. DHS also proposed to institute an exit pilot program for this population as well. In December 2008, DHS published final rules for these programs in: Changes to Requirements Affecting H-2A Nonimmigrants and Changes to Requirements Affecting H-2B Nonimmigrants. The pilot program establishes a land border exit registration procedure to record the departures of these temporary workers from the United States at the completion of their authorized work periods. The San Luis and Douglas, Arizona ports of entry were selected to be the sites for this land border exit pilot.

48. Some have proposed allowing Mexican and Canadian border authorities to collect exit information during their inspections at the land borders. This would seem to obviate the need to construct expensive infrastructure at the land border to accommodate exit inspections, and would increase the information sharing that is occurring at the border.

a. What is your assessment of this proposal?

We believe partnering with Canada or Mexico to use their entry as our exit is an option that we should continue to examine. However, such a strategy has not been successful to date, largely because of its dependency on the ability and willingness of our neighbors to participate.

DHS has proposed the idea of "their entry/our exit" to both Canada and Mexico with mixed results. In regard to Mexico, that country does not currently have a robust land port of entry infrastructure either in terms of technical or facility capabilities from which they can absorb additional requirements. They also do not currently collect biometrics at primary inspection facilities. Mexico would require significant financial, technical, facility, and human resources to significantly alter their collection processes. The Merida initiative will provide some funds towards enhancing their capabilities and infrastructure. We will continue to work with Mexico and examine options.

DHS has discussed this issue several times with Canada over the years, with particular emphasis on land border port of entry collection. It is important to recognize that Canada would also still require a significant enhancement of its information technology and facilities in order to absorb the additional collection requirements compared to their current processes. Most importantly, however, Canada has noted on previous occasions that its Charter of Rights prevents Canadian officials from taking fingerprints of landed immigrants and Canadians who are subject to US-VISIT. As these are most of the northern land border crossers, if they are unable to collect this data, the U.S. would not be able to use their collection as a mechanism to avoid the implementation costs.

b. Would you consider implementing a pilot program to test its feasibility?

Yes. We would be happy to discuss the opportunities for pilots with our neighbors.

49. DHS recently announced the appointment of Alan Bersin as DHS Assistant Secretary for International Affairs and Special Representative for Border Affairs. Bersin will be charged with, among other things, improving our relationship with our foreign partners and coordinating border enforcement programs.

a. What will be the relationship between US-VISIT and Mr. Bersin's new position?

I believe the Mr. Bersin will play an important role in assisting the Department's efforts in strengthening its border enforcement programs and coordinating cross-Departmental efforts. I further believe that US-VISIT plays an important role in the Department's border security and immigration efforts. If confirmed as Under Secretary of NPPD, I will encourage an open dialogue between NPPD's offices, including US-VISIT, and Mr. Bersin and his team.

- b. What actions will US-VISIT take to help Mr. Bersin improve our relationships with foreign partners?

It is my understanding that US-VISIT works closely with a number of foreign partners. I firmly believe that the Department's numerous offices and agencies must coordinate its activities in order to operate in the most efficient and effective manner. If confirmed as NPPD Under Secretary, I will work with US-VISIT to determine the most appropriate means to leverage the expertise at US-VISIT to assist the efforts of Mr. Bersin and his office.

50. DHS is currently working on a number of agreements with Visa Waiver Program nations to incorporate biometric data from other nations into our current border screening system. How does US-VISIT work with the Visa Waiver Program office to ensure that this data is incorporated as efficiently as possible into our screening process at the POEs?

US-VISIT works with the DHS Office of Policy, and its components the Office of International Affairs, Screening Coordination Office, and Visa Waiver Program Office to ensure that data collected from our foreign partners is appropriate and usable for US-VISIT.

Loran Program

51. The President's budget proposes eliminating the Coast Guard's LORAN program. The federal government has already invested \$160 million over the last 10 years to modernize LORAN-C in an effort toward deploying eLORAN as a national Position, Navigation, and Timing (PNT) back-up to GPS. GPS, because it uses a low-power satellite signal, is vulnerable to atmospheric interference and jamming. A national back-up system is therefore vital for mariners, aviators, and critical infrastructure operators. The decision to eliminate funding for the LORAN program appears to have been made without considering the value that eLORAN would provide as a national PNT back-up.

In 2006, DHS and the Department of Transportation jointly commissioned the Institute for Defense Analyses to conduct an assessment of the continuing need for the current LORAN infrastructure, as well as evaluate eLORAN as a potential next generation PNT back-up to GPS. The Institute created an Independent Assessment Team (IAT) to conduct this analysis, with a diverse group of senior decision-makers and experts from government, industry, and academia. The IAT reviewed about 40 previous reports and interviewed key stakeholders, industry representatives, and other relevant subject matter experts. In January 2009, the IAT released its report which unanimously concluded that eLORAN should serve as the national PNT back-up system for GPS and that U.S. LORAN infrastructure should be maintained until full eLORAN deployment.

- a. DHS has not finished its assessment of whether a single, national system is needed to back-up GPS. If confirmed, will you ensure that LORAN infrastructure is maintained

and funded until a final decision is made on whether eLORAN should serve as the national PNT back-up system for GPS?

The United States Coast Guard has been charged with the maintenance and operation of the LORAN System. Funding LORAN is not a responsibility of NPPD.

- b. NPPD has requested that the 18 national Critical Infrastructure and Key Resources (CIKR) sectors provide PNT requirements, supporting DHS' ongoing effort to determine if a single, national back-up system is needed for GPS. During her confirmation hearing, Deputy Secretary Lute stated that DHS expected NPPD's assessment to be completed by July 30, 2009. If you are confirmed, will you personally ensure this deadline is met?

The DHS Under Secretary of Management, Elaine Duke, has been tasked to assess whether there is a requirement for a national GPS back-up. She has requested a data call from Federal Agency's detailing their position, navigation and timing capabilities, requirements and assessment in the event of a loss of GPS-based services. NPPD is assisting the DHS Office of Management in reaching out and coordinating with the 18 CIKR sectors in regards to the data call, but NPPD is not conducting the actual assessment.

- c. There are multiple, limited systems that could back-up GPS, but these would not provide a national system with universal coverage for users. DHS is presently conducting a survey of critical infrastructure operators on their need for GPS back-up systems, but this has not been completed. Do you agree that it would be premature to discontinue the LORAN program before the Department reviews the operators' surveys and considers the comprehensive risk of not having a national system?

The Department of Homeland Security acknowledges the vulnerability of the nation's Global Positioning System (GPS) and is evaluating whether a national systemic backup is necessary. NPPD is not responsible for the LORAN program; however, the DHS Office of Management is currently assessing the need for a national GPS back-up. The DHS Office of Management will conduct an analysis of alternatives in the event Federal Agencies and Critical Infrastructure /Key Resource Sectors respond with requirements stating a need for a national backup capability.

- d. What is the estimated decommissioning cost of shutting down LORAN-C transmitting stations, and securing LORAN-C infrastructure nationwide?

The United States Coast Guard is responsible for the maintenance and operation of the LORAN-C system. It is my understanding that the United States Coast Guard is in the process of developing an estimate for the overall decommissioning costs for the system.

Maritime Security

48. One of the provisions of the SAFE Port Act of 2006, which this Committee authored, was the requirement to establish Interagency Operations Centers (IOCs) for port security at all high-priority ports not later than three years from the date of enactment. The Act authorized \$60 million each year from 2007 - 2012. In 2007, DHS identified the 24 high-priority ports that would require interagency operations centers and estimated that the entire project at the 24 ports would cost \$260 million, with an annual operating cost of \$3 million per center. What is the Department's timeline to fund and establish these first 24 IOCs? What role will IOCs play in helping prevent attacks on our nation's critical infrastructure and key resources?

I am aware of the provision in the SAFE Port Act requiring the stand-up of interagency operations centers. As I understand it, DHS intends to fully implement this provision; however, I have no details, at this point, on the timeline for the establishment of the IOCs. If confirmed, I will make sure that NPPD works to support this effort consistent with the goals and priorities of the program. The protection of critical infrastructure and key resources is best done through a collaborative approach. As such, I believe the IOCs can play an important role in securing the high-priority ports through collaboration and coordination with our Federal, State, and local partners.

49. It has been over a year since the Department issued its Small Vessel Security Strategy in April, 2008. What role, if any, has the Office of Risk Management and Analysis had in evaluating the small vessel threat, and drafting the subsequent implementation plan?

The goal of RMA is not to mandate that DHS components use a certain tool, analytical technique, or implementation plan to conduct their specific risk analyses. Instead, RMA is serving as the bridge to connect these existing efforts together and is building products and collaboration forums to better ensure they are harmonized moving forward.

Emergency Communications

50. Communications interoperability problems often create chaos when different units and levels of government simultaneously respond to a crisis. In 2006, Congress established the Office of Emergency Communications (OEC) to coordinate DHS's responsibilities on interoperability, develop a National Emergency Communications Plan, and conduct national outreach to foster interoperability among State, local, regional, and tribal governments. The National Communications System (NCS), also within NPPD, is the coordinator for Emergency Support Function 2 (Communications) under the National Response Framework. Other units within DHS also have significant responsibilities related to interoperability. For example, FEMA administers the Interoperable Emergency Communications Grant Program and has created a Disaster Emergency Communications Division to provide tactical emergency communications support to emergency responders at all levels of government. The Science and Technology Directorate is responsible for research, development, testing, evaluation, and standards related to interoperability.

- a. In its oversight of DHS, the Committee has found weak coordination among the various components within the Department responsible for interoperability. The DHS Inspector General (IG) also found only modest progress in this area within DHS in its 2008 report, "FEMA's Preparedness for the Next Catastrophic Disaster." How will you ensure that OEC and NCS properly coordinate with other entities within DHS to advance solutions to interoperability?

I strongly agree that close coordination among all DHS components with emergency communications responsibilities is required to achieve our Nation's National Security/ Emergency Preparedness and Interoperability communications goals. I will provide direction to NCS and OEC to fulfill their intended roles and missions as the lead integrators and coordinators of such DHS efforts. If confirmed, I will ensure that OEC, NCS and other NPPD components continue to coordinate on a regular basis and report regularly to me on their progress. OEC and NCS currently collaborate on a number of issues with respect to resilient and interoperable emergency communications. I will ensure OEC and NCS have the appropriate standard operating procedures for coordination with FEMA and other DHS components, thus providing a cohesive DHS approach.

In order to be effective, OEC and NCS must not only coordinate among and between themselves, but they must coordinate, collaborate and consult with the Nation's emergency responders and emergency response officials. Ongoing outreach efforts with our State, local, Territorial and tribal stakeholders, as well as with the private sector are an essential part to reaching this core constituency. I will strongly encourage continued collaboration between OEC, NCS, the Private Sector Office, the Office of International Affairs and the Office of Intergovernmental Programs to ensure mission bridging and efficiencies of efforts.

- b. Meeting immediate and long-term emergency communications needs also requires coordination among numerous federal agencies, including DHS, the Department of Commerce, and the Federal Communications Commission. In your experience, what is the key to a successful interagency effort involving numerous stakeholders?

I believe the key to a successful interagency effort involving numerous stakeholders is clear and concise communication, planning, and resource allocations among all parties. The most important among these is clear and concise communication; sharing information about goals and objectives leads to the development of a team that can advance the mission.

If confirmed, I will work to enhance emergency communications, and to strengthen inter- and intra-agency coordination.

- c. While OEC has made progress in recent months in hiring permanent staff, it remains heavily dependent on contractors. What steps will you take to strengthen OEC's organic capabilities and to ensure that OEC fulfills the role that the Committee

envisioned for it as the lead integrator for DHS's efforts to enhance emergency communications?

I believe that OEC has made significant hiring progress since its inception. It is my understanding that when the office stood up in April 2007, four federal employees were on board. As of May 1, 2009, OEC has 28 Federal employees on board, 9 other identified candidates in the hiring process, and is aggressively moving towards its full FY09 complement of 42 FTEs. In addition, the Office makes use of the Presidential Management Fellowship program, the DHS Policy Honors Fellowship program and detailee assignments to bolster its workforce.

To strengthen its organic capabilities, and to more effectively engage its stakeholders in the implementation of the National Emergency Communications Plan, OEC leads a number of advisory bodies and working groups, including the Emergency Communications Preparedness Center, the SAFECOM Executive Committee/Emergency Response Council, the Metropolitan Area Working Group, the Statewide Interoperability Coordinator Council, and others. These groups act as force multipliers by providing support, gathering input and disseminating information to and among emergency responders at all levels – Federal, State, territorial, tribal, local jurisdictions and national associations.

- d. The Integrated Wireless Network (IWN) project began in 2003 to create a nationwide, consolidated, interoperable wireless communications system for employees of DHS, the Department of Justice, and the Treasury Department. Despite the hundreds of millions of dollars spent, a December 2008 GAO report found that the program had failed due to a lack of leadership within the participating agencies. What is your understanding of the current level of collaboration and coordination among the Departments? Do you believe IWN can be revived to become an effective network to enable interagency interoperability? What are your plans for pursuing interagency coordination to ensure that employees of federal agencies are able to communicate with each other during a disaster?

While the Integrated Wireless Network (IWN) system in the Pacific Northwest has successfully transitioned from the pilot stage to a functional and user accepted system, the three partner agencies have jointly determined that IWN is not a viable nationwide solution. As such, the three partners signed a new Memorandum of Understanding in January 2008 establishing a partnership agreement entitled the Joint Wireless Program.

However, I believe the basic IWN concept of shared systems and resources can be implemented effectively within the framework of the Emergency Communications Preparedness Center. Through this Center, DHS and the Office of Emergency Communications will continue to work with other Federal departments and agencies, including the Departments of Justice and the Treasury, as well as state and local

agencies to identify potential partnerships and to leverage common resources and infrastructure.

IV. Relations with Congress

51. 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.

52. 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.

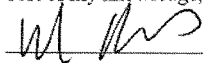
V. Assistance

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

In an effort to be as forthright and responsive as possible to the Committee in the time available, I have participated in normal pre-confirmation consultations with DHS staff, including officials in the National Protection and Programs Directorate. These consultations were used to inform my knowledge regarding the background, current operations and potential policies for the Department. However, and in all cases, these answers are my own, and are based on my understanding and consideration of the information provided to me.

AFFIDAVIT

I, RAND BEERS, 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 11th day of May, 2009.


Notary Public

Stuart A. Connolly
Notary Public, District of Columbia
My Commission Expires 1/1/2012



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

April 23, 2009

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 Rand B. Beers, who has been nominated by President Obama 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 agency concerning any possible conflict in light of its functions and the nominee's proposed duties. Also enclosed is an ethics agreement outlining the actions that the nominee will undertake to avoid conflicts of interest. Unless a date for compliance is indicated in the ethics agreement, the nominee must fully comply within three months of confirmation with any action specified in the ethics agreement.

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

Sincerely,

Robert I. Cusick
Director

Enclosures - REDACTED

April 22, 2009

Robert E. Coyle
Designated Agency Ethics Official
Department of Homeland Security
Washington, DC 20528-3650

Dear Mr. Coyle:

The purpose of this letter is to describe the steps that I will take to avoid any actual or apparent conflict of interest in the event that I am confirmed for the position of Under Secretary for National Protection and Programs, Department of Homeland Security.

As required by 18 U.S.C. § 208(a), I will not participate personally and substantially in any particular matter that has a direct and predictable effect on my financial interests or those of any person whose interests are imputed to me, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1), or qualify for a regulatory exemption, pursuant to 18 U.S.C. § 208(b)(2). I understand that the interests of the following persons are imputed to me: any spouse or minor child of mine; any general partner of a partnership in which I am a limited or general partner; any organization in which I serve as officer, director, trustee, general partner or employee; and any person or organization with which I am negotiating or have an arrangement concerning prospective employment.

In January 2009, I resigned from my position of President and Chairman of the Board of National Security Network and President and Board member of National Security Initiative. For a period of one year after my resignation from each of these entities, I will not participate personally and substantially in any particular matter involving specific parties in which either of these entities is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

Since February 2004, I have served as an Adjunct Professor for Harvard University. The last course I taught ended in December 2008. For a period of one year I will not participate personally and substantially in any particular matter involving specific parties in which Harvard University is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d).

Finally, I understand that as an appointee I am required to sign the Ethics Pledge (Exec. Order No. 13490) and that I will be bound by the requirements and restrictions therein in addition to the commitments that I have made in this or any other ethics agreement.

Sincerely,



Robert R. Beers

Senator Daniel K. Akaka
Additional Questions for the Record
Nomination Hearing of Rand Beers
June 2, 2009

1. You stated in response to the Committee's policy questions that consideration of a potential policy's impact on privacy and civil liberties should be included in risk management decisions.

How will the National Protection and Programs Directorate (NPPD) ensure that privacy and civil liberties are integrated into those decisions at the Department of Homeland Security (DHS)?

The DHS approach to integrated risk management acknowledges that decisions are rarely purely risk based, but instead should be risk informed. Risk-informed decision making is the determination of what actions to take predicated on the assessment of risk and the expected impact of those actions on that risk, as well as on other factors related to the context of the decision, such as the effects of a risk mitigation strategy on privacy and civil liberties.

In January, the Department released an Interim Integrated Risk Management Framework. The Department is now in the process of drafting the final Integrated Risk Management Framework for DHS, scheduled to be finalized this fall, which will incorporate discussion on the potential of impacts to policies from risk management decisions, including specific language on privacy and civil liberties.

2. Homeland security is a national mission that involves a number of Federal agencies, all levels of government, the private sector, and citizens. As you know, DHS is using a risk management framework called Risk Assessment Process for Informed Decision-Making (RAPID) to provide a common approach for decision-makers to assess component programs. It does not appear that other stakeholders are using consistent risk-based, decision-making approaches.
 - a. How does DHS intend to work with stakeholders to ensure a more consistent framework for risk assessment?

One of the studies being conducted as part of the Quadrennial Homeland Security Review (QHSR) is a review of the concept of conducting a homeland security national risk assessment to guide strategic prioritization across the homeland security community. The study is intended to answer the question of: What process and methodology should be used to assess all-hazard national homeland security risk, and how will that assessment inform strategic prioritization and decision-making?

In addition, to the QHSR effort, DHS, led by the Federal Emergency Management Agency and the Office of Risk Management and Analysis, is currently working with State and local governments and private sector stakeholders to revise the "risk management" target capability. The risk management target capability effort is designed to provide guidance and identify resources to help State and local governments enhance their capability to make risk-informed decisions amongst their homeland security needs in a consistent manner. It also will provide performance objectives against which jurisdictions and DHS can measure risk management progress in a standardized manner.

b. How will input from stakeholders be incorporated into that process?

Both of these processes are being conducted transparently with community-wide involvement. As part of the QHSR, stakeholders will be asked to provide thoughts, positions and ideas on possible solutions and comment on issues under consideration during the study through a systematic process. In addition, Federal interagency partners will be part of the QHSR.

The target capability definition will be driven by State and local government feedback, and include private sector participation. This summer, FEMA is hosting regional workshops led by RMA to define the target capability and develop performance objectives. In addition, DHS is exploring options for broader community feedback through national homeland security associations and the use of organizations which partner with FEMA.

3. DHS's Fiscal Year 2010 budget proposes moving the Federal Protective Service (FPS) from Immigration and Customs Enforcement (ICE) to NPPD. Recently, the DHS Inspector General identified a number of weaknesses in the FPS contract security guard program, including inconsistent selection practices and a lack of oversight by FPS. Currently, FPS relies on the ICE Consolidated Contract Group for contract guard procurement and other acquisitions.

a. If FPS is moved, what steps will you take to minimize disruptions to FPS operations and procurement during its transition to NPPD?

Since the rollout of the President's FY10 Budget Proposal on May 7, and announcement of the proposed shift of the FPS from ICE to NPPD, a senior group from all three organizations has met to exchange initial information and establish communications, in the event that Congress moves FPS in the Department's annual appropriations act. This group has recently established an FPS Transition Senior Working Group consisting of senior leadership from ICE, NPPD and FPS as Co-Chairs with reporting of more than a dozen staff-level working groups, which includes an Operations Working Group and Acquisitions Working Group. The purpose of this FPS Transition Senior Working Group will be to work through the transition process and produce an FPS Transition Plan, anticipating a favorable response from Congress. This document is intended to serve as a

planning tool and will include milestones for implementation and can be adjusted accordingly and as necessary.

b. How will you address the procurement and acquisitions issues raised by the DHS Inspector General?

In its response to Inspector General Skinner, FPS identified measures it has taken and others that it will take to address the three procurement and acquisitions issues identified in the OIG Report. For example, FPS and ICE completed a full review and revision of the Request for Quotes (RFQ) and Request for Proposals (RFP) templates this year. FPS, ICE and NPPD will continue their commitment to identify and refine existing templates and to develop new templates and standardized policies/procedures within the contract guard acquisition program to ensure contracts are awarded in the government's best interest. Acknowledging its contracting resource constraints, FPS identified approaches it has taken to provide an ongoing assessment of evaluations being conducted to ensure that they meet or exceed established thresholds for quality and timeliness. In addition, FPS has expanded training, as well as the development and use of standardized templates and evaluation guides that has resulted in a streamlined process and a more knowledgeable workforce and an increased ability of regional personnel to conduct technical evaluations. These and other actions submitted in response to the DHS/OIG final report titled, "Federal Protective Service Contract Guard Procurement and Oversight Process", will be carefully reviewed by the FPS Transition Senior Working Group to ensure that the actions proposed and those implemented will ensure that FPS consistently solicits and awards guard contracts that are in the government's best interest.

Senator Susan M. Collins
Additional Questions for the Record
Nomination Hearing of Rand Beers
June 2, 2009

1. I understand that the Department is continuing its assessment into whether a single, national back-up system is needed for GPS. This assessment is due to be completed no later than July 30, 2009, with a final decision on eLORAN's future expected within days of this deadline. In your pre-hearing policy questionnaire you stated that, "NPPD is assisting the DHS Office of Management in reaching out and coordinating with the 18 Critical Infrastructure and Key Resources (CIKR) sectors in regards to the data call, but NPPD is not conducting the actual assessment."

Can you update the Committee on the status of this data call? Specifically, which Critical Infrastructure and Key Resource sectors have responded to the data call, and what information have they provided?

The current data call is being administered by the Department's Under Secretary for Management. Upon reaching out to the Under Secretary for Management's lead on this effort, I was informed that at this point DHS has not received any responses from the 18 CIKR sectors on the GPS backup capabilities data call. The sectors have until June 19, 2009, to respond to the data call. The Department will continue to work with the Committee on this issue, and will follow-up with the Committee upon completion of the data call and analysis of the results the end of July 2009.



The Honorable Joseph Lieberman
Chairman
Committee on Homeland Security
and Governmental Affairs
U.S. Senate
Washington, DC 20510

The Honorable Susan Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
U.S. Senate
Washington, DC 20510

Dear Senators Lieberman and Collins:

I am writing to offer my unequivocal support for Rand Beers' nomination as Under Secretary of the Department of Homeland Security. Rand is quite simply a public servant of the highest order. The skills and expertise he has demonstrated over his unique professional career make him perfectly suited to run the DHS National Protection and Programs Directorate (NPPD) at a truly critical time in our nation's history.

While his resume stands as a testament to a diverse and patriotic career, I can personally attest to Rand's professional commitment and abilities. I had the pleasure of working with Rand during my time as Assistant Attorney General running the Criminal Division of the Department of Justice. In this capacity, I oversaw Justice's international narcotics portfolio, while Rand was serving as Assistant Secretary for International Narcotics and Law Enforcement Affairs at the State Department. I will state wholeheartedly that Rand is an outstanding manager and a genuine expert in the fields of Homeland, National, and International Security.

As I have personally discussed with you both, cyber security, critical infrastructure protection, and risk management are central to the threats currently facing our country. You have appropriately identified these areas as key priorities for the committee moving forward under your leadership. I believe that nominating Rand to run the very directorate charged with these issues demonstrates that this Administration and Secretary Napolitano recognize the importance of addressing such critical vulnerabilities.

As you both know, I have the utmost respect for this committee, and for your diligent oversight of DHS. To that end, I urge swift confirmation of Rand Beers – so that you have a partner of unquestionable quality in your endeavor to protect our nation.

Sincerely,

Michael Chertoff
Co-Founder and Managing Principal

1110 VERMONT AVENUE NW, SUITE 1200
WASHINGTON, DC 20005
T. 202.649.4360 F. 202.330.5505
WWW.CHERTOFFGROUP.COM

