S. Hrg. 113–142

NOMINATIONS OF HON. STEVAN E. BUNNELL AND SUZANNE E. SPAULDING

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

NOMINATIONS OF HON. STEVAN E. BUNNELL TO BE GENERAL COUNSEL, U.S. DEPARTMENT OF HOMELAND SECURITY AND SUZANNE E. SPAULDING TO BE UNDER SECRETARY FOR NATIONAL PROTECTION AND PROGRAMS, U.S. DEPARTMENT OF HOMELAND SECURITY

SEPTEMBER 18, 2013

Available via the World Wide Web: http://www.fdsys.gov/

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

U.S. GOVERNMENT PRINTING OFFICE
85–507 PDF WASHINGTON : 2014

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan	TOM COBURN, Oklahoma
MARK L. PRYOR, Arkansas	JOHN MCCAIN, Arizona
MARY L. LANDRIEU, Louisiana	RON JOHNSON, Wisconsin
CLAIRE MCCASKILL, Missouri	ROB PORTMAN, Ohio
JON TESTER, Montana	RAND PAUL, Kentucky
MARK BEGICH, Alaska	MICHAEL B. ENZI, Wyoming
TAMMY BALDWIN, Wisconsin	KELLY AYOTTE, New Hampshire
HEIDI HEITKAMP, North Dakota	JEFF CHIESA, New Jersey

RICHARD J. KESSLER, *Staff Director*
JOHN P. KILVINGTON, *Deputy Staff Director*
DEIRDRE G. ARMSTRONG, *Professional Staff Member*
MARY BETH SCHULTZ, *Chief Counsel for Homeland Security*
STEPHEN R. VIÑA, *Deputy Chief Counsel for Homeland Security*
MATTHEW R. GROTE, *Senior Professional Staff Member*
JOHN G. COLLINS, *Professional Staff Member*
DEANNE B. MILLISON, *Counsel*
KEITH B. ASHDOWN, *Minority Staff Director*
CHRISTOPHER J. BARKLEY, *Minority Deputy Staff Director*
DANIEL P. LIPS, *Minority Director of Homeland Security*
SARAH BETH GROSHART, *Minority Counsel*
LAURA W. KILBRIDE, *Chief Clerk*
LAUREN M. CORCORAN, *Hearing Clerk*

CONTENTS

WITNESSES

WEDNESDAY, SEPTEMBER 18, 2013

NOMINATIONS OF HON. STEVAN E. BUNNELL, AND SUZANNE E. SPAULDING

WEDNESDAY, SEPTEMBER 18, 2013

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

The Committee met, pursuant to notice, at 9:32 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Thomas R. Carper, presiding.

Present: Senators Carper, Coburn, Johnson, Ayotte, and Chiesa.

OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. The hearing will come to order.

I am happy that we are here, and have our nominees here. We welcome you. We got to meet some of your families—parents, spouses, children—and it is just a joy to meet them and a joy that they can be here to support both of you. I would say to the parents that are here, thank you for infusing the kind of values in this young woman, this young man, and inspiring them and encouraging them to serve our country in a variety of capacities. Usually, kids do not turn out well unless their parents had something to do with it, so moms and dads sitting in the audience, nice work. Nice work.

Before I turn to Dr. Coburn for any comments that he might want to make, I want to just give a fairly brief opening statement and we will get started.

But the other thing I want to do, we have a Bible study that meets every Wednesday morning. I do not usually get to go because it is pretty early, eight to nine. I am usually on a train coming down. Senator Johnson is often there and a number of our other colleagues. We were reminded this morning of the folks who have literally laid down their lives in service to our country and were tragically gunned down just a couple days ago.

I just want to start this hearing today with a moment of silence in their memory and thanks and gratitude to them and in a sense of one, in unity with their families. Will you just do that. [Moment of silence.]

Thank you.

Well, one of my hopes, one of my aspirations is that we can, by working together, learn as much as possible from the tragedy that occurred 2 days ago so that we can prevent or at least reduce the likelihood of those kinds of tragedies occurring again in the future. We know that the Department of Homeland Security (DHS) is

going to be doing its part to learn from this incident, the sadness, and to do its best to ensure we do not let it happen again.

Today, we consider the nominations of Stevan Bunnell, President Obama's choice to serve as the General Counsel of the Department of Homeland Security, and Suzanne Spaulding, the President's nominee to be Under Secretary for the National Protection and Programs Directorate (NPPD).

These positions, as we know, are extremely important to not just the Department, I think, but to the security of our Nation and its people. The National Protection and Programs Directorate, for example, is responsible for securing our Nation's critical infrastructure from cyber attacks. The General Counsel serves as the Secretary's chief legal advisor and ensures that the Department's activities are consistent, one, with the Constitution, and two, with the laws that we pass here in Congress.

I know that my colleagues and I on the Committee are very pleased to see the President has put forth nominees to fill the leadership vacancies in these critical components. The Administration has made some recent progress, much needed, toward filling a number of vacancies in the Department, and from what I understand, the nominations are pending for four of the eight Senate-confirmed vacancies at the Department of Homeland Security. Of course, that still leaves four positions without even a name put forward, including the Secretary and Inspector General (IG). It is imperative that we get all these vacancies filled as quickly as possible.

As I said before, the confirmation process is a shared responsibility. The Administration has the responsibility to give us the names of excellent people—I think the President has today—people who are hard working, who are honorable, capable people who can provide strong leadership, not just at the Department of Homeland Security but across our government.

My colleagues and I here in the Senate have an obligation of our own to exercise our advice and consent responsibilities in a judicious but timely manner. If a nominee is qualified, we need to move him or her quickly.

This morning, we have before us two people who I believe are very well qualified. Stevan Bunnell has over 25 years of experience practicing law, and for 17 of those years, he served in positions of increasing responsibility as a prosecutor and supervisor at the Department of Justice (DOJ), including as Chief of the Fraud and Public Corruption Section and Chief of the Criminal Division at the U.S. Attorney's Office in Washington, DC.

In addition to working with a variety of law enforcement agencies on complex criminal cases, it is my understanding that Mr. Bunnell has also worked closely on national security issues with someone we are all very familiar with, and that is Michael Chertoff, then Assistant Attorney General in the Department of Justice, later Secretary for the Department of Homeland Security. Later, Mr. Bunnell left the government for private practice. He is currently serving as the Managing Partner of the law firm O'Melveny and Myers in Washington, DC.

Sitting beside him, to his left, to our right, is Suzanne Spaulding. She comes to us with a rich background in both government service

and work in the private sector. She is currently serving as the Acting Under Secretary for the National Protection and Programs Directorate. Before that, she served as Deputy Under Secretary in the Directorate.

Ms. Spaulding's distinguished career has also included positions as the General Counsel for the Senate Select Committee on Intelligence, Staff Director of the House Permanent Select Committee on Intelligence, and as an attorney for the Central Intelligence Agency (CIA). She has also had several years of experience in private practice.

Sitting in the seat that Mr. Bunnell is sitting was Jane Harman, who sat in that seat last week on the anniversary of September 11, 2001, and had wonderful things to say about you, Suzanne, and your service.

In her current post at the Department of Homeland Security, Ms. Spaulding has brought a direct and engaged management approach to some of the Department's most important missions.

Over the course of their respective careers, both of our nominees have shown themselves to be natural leaders. In addition, both have become widely respected by their peers for their intellect, for their professionalism, and for their integrity. I believe these are the types of qualities we want to see—need to see—in our government leaders.

I would like to ask for unanimous consent to enter into the record all the letters of support[1] we received that speak to the wonderful attributes of our nominees.

To conclude, I just want to thank both of our nominees for their willingness to continue to serve—our Nation in these important responsibilities, important posts, and also again to thank their families for raising them and for their willingness to share them with all of us. We know that public service is not always easy. It is rarely easy. My dad used to say the hardest things to do are the things most worth doing, so this is hard work and we are grateful that you are willing to do it and we thank your families again for their commitment to our Nation and for being here with us all today.

With that, I turn to my friend, Dr. Coburn, for any comments he might want to add, and then we are going to recognize some of our introducers of these folks. Please, Tom.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Thank you. I am going to go out of my normal realm and actually read my opening statement today because it covers some areas that I want to make sure are emphasized.

First of all, I want to welcome you. I think we have two very well qualified candidates, and I talked with the Acting Secretary yesterday and assured him I would do everything I could to move these nominations to the Senate floor.

Leadership vacancies are the biggest challenge right now facing the Department of Homeland Security. This Committee held a hearing last week looking at the lessons learned and challenges facing the Department. We heard from former Secretary Ridge and other former senior officials about the many and multiple chal-

[1] Letters of support appear in the Appendix on page 240.

lenges that DHS faced, from questions about congressional oversight to mission creep and successful integration of the Department and its components.

A clear take-away from that hearing was that it is going to require real leadership to address these problems and create a well-functioning Department for the next 10 years. And, of course, the biggest problem there is the vacancies, the 15 key vacancies, eight of which are Senate approved, seven of which are not. If DHS is going to address its many challenges and become a well functioning Department with great morale, it will require strong and effective leadership atop the Department and at each component, each office, and each directorate.

I am hopeful that our two nominees under consideration today will earn the Committee's support and be confirmed. Each of you has an impressive resume and experience and knowledge that make you well qualified for the positions to which you have been nominated.

To Ms. Spaulding, I have really appreciated our meetings, both at DHS and in my office, and the candid conversations that we have had about the challenges.

Mr. Bunnell, I have reviewed your background and your questionnaires, and I understand that you are more than well qualified for the position to which you have been nominated.

But by earning the trust and the support of our Committee, we ask for your word and assurance that we will be partners in working together to fix the Department. Conducting oversight is our job, and asking questions on behalf of the American people is one of our Committee's main responsibilities.

Unfortunately, in my experience to date, over the last 8 years, 8½ years, DHS too often does not cooperate with our oversight requests and many times has undermined our ability and what could be a collaborative process to identify and fix problems.

For example, when the Permanent Subcommittee on Investigations was doing our investigation into the Fusion Center program, DHS seemed to use every available tool that they could, including weak legal arguments, to drag out the process and undermine the oversight process. The result was significant in our investigation, which ultimately found some significant problems. And that was a lose-lose for DHS, the Congress, and, frankly, the American people who are paying for the programs. Instead of spending 2 years fixing the problem and figuring out how DHS's intelligence program could yield better value for the American taxpayer, we were stuck in absurd legal debates over document production.

In other cases, I have asked basic questions and did not receive straight answers from the Department. For example, during the immigration reform debate, I asked the Secretary whether or not she could share with me her border sector specific security plan and provide a congressionally mandated border security status report. The initial report was due in Congress in February 2012, which we still do not have. And we still do not have a sector specific border security plan. And the information I got was not helpful at all. So, our Committee in the Senate had to vote on an immigration bill without the full knowledge and full input of the people who have most of the knowledge.

Today, I ask you to be partners with our Committee and to pledge to be cooperative with our Committee and the Congress in the oversight process.

In the conversations I have had personally with Ms. Spaulding, I have shared we are not in "gotcha" mode. The problems are too great to play politics with what is going on at Homeland Security.

And, Mr. Bunnell, as General Counsel, you have the responsibility of overseeing how the Department and its components will respond to our oversight requests. I ask you to commit today to being supportive and cooperative and transparent with those requests.

The NPPD is a directorate with a troubled track record. We have had those discussions. The Committee and Congress have had serious questions about the key initiatives of this directorate, such as the Chemical Facility Anti-Terrorism Standards (CFATS) program for chemical facility security, and last night, I got an update. We have 25 of some 5,000 now approved. We have not had one onsite visit. We have 25 approved. And none of those are really approved because they have not been checked against the security lists that we maintain. So, even though I know we have a good person in there now, that is a significant problem.

The other thing that came to my mind was what I have heard in terms of pipeline and what the Transportation Security Administration (TSA) is doing in terms of withdrawing on pipelines, which are a vulnerable area for our country. So, I will talk with you specifically about those things and how we address them.

We also have questions about some key issues that you will be responsible for moving forward on which we will discuss in the questions and answers, and I will not go into those now.

I will just close my opening statement by thanking you both for your willingness to serve. I look forward to your testimony and I look forward to a great relationship of collaboratively working to solve the problems.

Tom and I have a great relationship. We can move a lot of things to help you, and we can move a lot of things through this Committee that will help streamline things and help you actually do your job. But we cannot do it unless you share information with us. So, for example, on the Integrated Product and Process Development (IPPD), you have given us some information, but the people that are cooperating with you in the private sector, it is not classified information but yet we cannot get a list of those people so we can talk with them about what their assessment is of what you are doing. So, doing good oversight means we actually do good oversight. So I will be visiting with you.

I thank you again for your service and look forward to your testimony.

Chairman CARPER. Dr. Coburn, thanks very much.

I want to welcome Senator Johnson and Senator Ayotte. Thank you for being here again. You are very faithful here. I am grateful for that.

Senator Warner, good morning. Senator Kaine, nice to see you, third time this morning. I am going to call on you, if you will, to introduce one of our nominees, and then I will call on Mr.

Wainstein to handle the honors for Stevan Bunnell. Mark Warner, welcome. How are you?

OPENING STATEMENT OF SENATOR WARNER

Senator WARNER. Fine, Mr. Chairman. I thank you and Ranking Member Coburn, Members of the Committee.

Let me make one quick editorial comment, agreeing with Senator Coburn. Not just at DHS but across the Administration, there are way too many positions unfilled at this point, and as a former Governor, the idea that you would be this far into your term and not having your whole legislative team filled out, or your management team, is something that needs to be addressed.

You get an opportunity in this job to come out and introduce a number of folks, oftentimes from your State. It is rare that you get to come by and introduce and present somebody who has been a friend of over 30 years. Suzanne Spaulding and her husband, Gary, and their kids, Max and Charlotte, are dear personal friends of Lisa and I, social friends, business friends, political friends, and I come here unreservedly endorsing Suzanne Spaulding to this Committee for her, I think, very appropriate nomination as Under Secretary for National Protection and Programs Directorate at DHS.

Suzanne's parents both served in the military. Her brother, Doug, is here. This is a family who has been all about public service throughout her whole career. She is somebody, as I have tried to learn issues around national security and intelligence, that I have turned to in the Senate, but she is also, when I was Governor, someone I appointed to the Commonwealth Panel, where she advised me on issues that are at the State level very similar to what she will be working with this Committee on at the national level.

She also, as I think the Chairman pointed out, has a broad bipartisan background. She worked for a long time for former Chairman and Senator Arlen Specter, who was a tough taskmaster on issues. She also worked for previous Virginia Governor Jim Gilmore on his Committee on Terrorism. Clearly, this kind of background, bipartisan background, her service with the CIA, her service in the private sector, I think all recommend her to the Committee.

As, I think, Senator Coburn has indicated in his comments, I think you will find someone in Suzanne that will be that kind of active, engaged; recognizing the very important role that Congress plays, having had a great deal of her career not being on an Administration side but sitting behind members such as yourselves, trying to get out of previous Administrations the kind of information that I think you and we appropriately should and deserve to receive as members of oversight panels.

Clearly, in the cyberspace, there is enormous work to be done. I again want to commend the Chair and the Ranking Member for moving forward on this issue. I think there is a new sense that this is an issue area that we cannot continue to punt on. We have a lot of overlapping jurisdiction, but under your leadership and the other Committees, a couple of them which I participate on, I think we are going to get something done. Suzanne's role at DHS in coordinating those activities, I cannot think of an area that is of more importance.

So, from a professional endorsement, from a personal endorsement, from a family who has been all about service, I unreservedly recommend Suzanne Spaulding for this position and I hope the Committee will act on her nomination in a judicious and speedy manner.

Thank you, Mr. Chairman.

Chairman CARPER. Thank you. That is a great introduction and recommendation. We value it. Thank you very much. I know you have a lot on your plate today, so feel free to depart if you——

Senator WARNER. I want to make sure my dear colleague and the junior Senator does not mess up his recommendation, as well, so I will listen to that first and then I will get out of the way. [Laughter.]

Chairman CARPER. I was watching his lips move while you spoke, so—— [Laughter.]

You guys have been doing this for a while. I do not think he will mess up.

Senator Kaine. Governor Kaine. Welcome.

OPENING STATEMENT OF SENATOR KAINE

Senator KAINE. Thank you, Mr. Chairman and Ranking Member Coburn and Committee Members. It is a treat.

This is a real example of the best and brightest, being here for Suzanne, and I think we often have hearings where it is about the best and brightest, but I do not remember doing one where I thought it was the best and brightest who was so particularly suited for this particular position.

To begin, as my friend, Mark, mentioned, her family has a great family career in public service, both in civilian public service and also service in the military, her parents, her brother, her sister, and Suzanne. We may not do all we need to do to honor the service of those who serve the country in both military and civilian capacity. We learned to our horror 2 days ago that their sacrifices, including sacrifices that you do not expect to happen, but this family has sacrificed for public service in some really notable ways and I begin there.

And, second, Mark talked a bit about her background. Suzanne has worked for 25 years in this field of trying to advocate for the Nation's security in the private sector and in the public sector, in the public sector at the Federal level and at the State level. At the Federal level, in the executive and in the legislative. In the legislative for Democrats and Republicans and for the Senate and House. She has touched this issue from virtually every angle and made it her life's work and her life's passion.

And in serving in this acting capacity, she has earned the confidence of this Administration and she has also earned the confidence of two previous DHS Secretaries, Secretaries Chertoff and Ridge, who have strongly weighed in on her behalf, and I think all that speaks very well of her nomination and I urge her to be considered favorably and promptly.

Chairman CARPER. I want to thank you both. If you need to go, please do. We value your presence. We value your kind words, generous words about Ms. Spaulding and her nomination.

I am going to turn now, if I could, to Ken Wainstein. I am going to ask you to turn on your microphone so that we will be able to hear you. But I understand that you are a partner at the law firm of—first of all, I understand you are a friend, maybe a longtime friend, of a former colleague of our nominee, Stevan Bunnell, and I understand you are a partner at the law firm of—I want to say it is Cadwalader—how do you pronounce it?

Mr. WAINSTEIN. Cadwalader Wickersham and Taft.

Chairman CARPER. Cadwalader Wickersham and Taft. At least I got the "Taft" right. That is good.

Previously, he served as an Assistant to the President for Homeland Security and Counterterrorism, for President George W. Bush. Mr. Wainstein also served as the first Assistant Attorney General for National Security at the Department of Justice and as the United States Attorney in Washington, DC. That is a great resume yourself.

We are delighted that you are here to introduce your friend, your former colleague, Stevan Bunnell. Please proceed.

OPENING STATEMENT OF MR. WAINSTEIN

Mr. WAINSTEIN. Thank you, Chairman Carper, Ranking Member Coburn, Members of the Committee. It is an honor to appear before the Committee today and to introduce my friend, Steve Bunnell.

As the Chairman just pointed out, I served for over 20 years as a lawyer in Federal service in a variety of different positions, and in all of those positions, I had the opportunity and the privilege to work closely with Steve Bunnell.

But before providing my personal perspective on Steve, I would like to take a moment to just go through his resume and his objective qualifications for this job.

A Phi Beta Kappa graduate from Yale University and then Stanford Law School, a prestigious clerkship with a highly respected D.C. Circuit Court judge, 5 years of stellar service as one of the standout line prosecutors in the U.S. Attorney's Office in D.C., public corruption prosecutor, counsel to Assistant Attorneys General for both the Clinton and the Bush Administrations, Chief of the whole Criminal Division at the U.S. Attorney's Office, and then ultimately managing partner at O'Melveny.

So, those are Steve's pretty incredible credentials on paper. Let me now explain the reasons why those credentials and Steve's character add up to what I think is the ideal nominee for the DHS General Counsel position.

First and foremost, Steve is, quite simply, an excellent lawyer, one of the very best I have ever worked with. His analytical skills, his judgment are exceptional and they have been honed through years of wrestling with tough issues of law and fairness as a line prosecutor and also tough issues of national security policy when he served as a high-level Justice Department official. He has always been the first person I have sought out whenever I have needed sound and honest advice about a tough situation.

Besides being a tremendous legal talent, Steve has exceptional leadership skills, skills that, as Senator Coburn pointed out, are absolutely critical in a Department like DHS, but particularly important for a General Counsel who is responsible for managing an

extended group of DHS lawyers across a wide spectrum of agencies and also responsible for representing the Department in the interagency process with strength and credibility.

At every step of his career, Steve has shown himself to be a natural leader who sets an example for the rest of his colleagues.

He has also proven himself a true government professional in the best sense of the word. In other words, he has shown himself to be a completely apolitical straight shooter, someone who always subordinates political interests to the mission and to the needs of the agency that he serves and his country, and that is a reputation that I think is well reflected in the letters of support that he has received from all parts of the political spectrum.

Last and most importantly, Steve is a man of honor. He is a man who has got the personal character one would want in such an important and sensitive position. He is universally, and I mean that, universally respected and admired by all those who have ever worked with him, from Attorneys General he has worked with, to Deputy Attorneys General of both parties, to the counsel and associates at O'Melveny who have flourished under his inclusive management style.

He has earned that admiration, in part, by just good old smarts and hard work, but also because he has always conducted himself in a way that exemplifies the qualities of decency, integrity, and fidelity to public service. His willingness to step out of a highly successful law firm practice right now and into DHS is just the most recent example of his selflessness and sense of duty.

In sum, I cannot think of a better person to assume this important position and I am confident that Steve will serve with honor and with distinction and that the people of our country will be more secure, both in their safety and in their civil liberties, thanks to Steve's service as General Counsel. I, therefore, give him my unqualified recommendation and urge the Committee to endorse him unanimously.

Thank you, Mr. Chairman.

Chairman CARPER. Thanks for those great words. I think we already had high regard for him before you spoke, and watching you speak, I was watching his parents and their heads were going up and nodding "yes" in agreement. I know they are proud.

Should we go ahead and allow Mr. Bunnell and Ms. Spaulding to actually give their statement? We do not do that, do we? Do we not swear them in? My script did not look right, so we are going to do it this way. We are going to swear you in.

I ask you both to stand. I will put you under oath, and then we are going to ask you to proceed with your statement. Thanks. Would you rise and raise your right hand, please, and I would ask you this question.

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

Mr. BUNNELL. I do.

Ms. SPAULDING. I do.

Chairman CARPER. All right. Please be seated.

Senator COBURN. May I make a clarification to my opening statement? I said six. It was 6 percent on the CFATS, not six. Thank you.

Chairman CARPER. Good. All right, Mr. Bunnell. You may proceed with your statement and please introduce your family and friends. We have had a chance to meet them in the anteroom, but please feel free to introduce them for us, too, and then we will turn to Ms. Spaulding. Thank you. Please proceed.

TESTIMONY OF STEVAN E. BUNNELL,[1] NOMINATED TO BE GENERAL COUNSEL, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BUNNELL. Thank you, Mr. Chairman, Ranking Member Coburn, Members of the Committee.

Let me also thank my good friend, Ken Wainstein, for his very kind introduction today and his support throughout the confirmation process.

It is an honor for me to be here today as the nominee to be General Counsel of the Department of Homeland Security. I thank the President for his confidence in me and I thank the Committee for moving forward judiciously and expeditiously on this nomination, and Suzanne's nomination, as well.

I would also like to thank and recognize the members of my family who are here today, my wonderful wife, Laura, who has always been so supportive of my passion for public service despite the many sacrifices it imposes on her and her own successful law practice. I do not know how she does it all, but I do know that she is truly my better half.

We have two sons, Philip, who is in college in California and could not be here today, and Daniel, who is here and is a senior in high school. Philip and Daniel are not only my pride and joy, they are also a reminder to me that the work being done on homeland security today is not just about keeping us safe in the present, it is about building a foundation for a safe, secure, and resilient future for the next generation and making sure that future generations enjoy not only physical security, but also the fundamental rights and freedoms that we all hold dear.

I am grateful that my parents, Fred and Alice Bunnell, are here today. Both my parents are retired teachers. They instilled in me and my sisters a strong ethic of service, of giving back. They continue to be an inspiration to me.

I would also like to thank my two sisters, Becky, who works for the Centers for Disease Control (CDC) in Atlanta and is here today, and my other sister, Ann, who is a social worker in Chicago. I owe them a special thanks, I think, for helping me, as only siblings can, to learn at a young age how to share toys, share chores, and work together with people I do not command or control. [Laughter.]

Those sibling experiences provided a foundation for skills that have served me well in life so far and are skills I am sure I will continue to rely on if I am lucky enough to be confirmed.

[1] The prepared statement of Mr. Bunnell appears in the Appendix on page 49.

Finally, I would like to thank my wife's parents, Rod and Carla Hills, for being here today and for being role models, not just for me, but for anyone who aspires to serve our country with distinction.

Chairman CARPER. Did your mother-in-law not have a job in one of those Bush Administrations a while back?

Mr. BUNNELL. She has had so many distinguished jobs, sir, I would not be able to list them all——

Chairman CARPER. All right. It is nice to see all your family, but I especially would recognize her and her service. Thank you.

Mr. BUNNELL Thank you. Thank you, Mr. Chairman. I think they serve as a model for anyone who aspires to serve at the highest levels of government with honor and distinction.

I am excited about the possibility of returning to public service. I believe my prior experience in government and my more recent experience managing lawyers in a leading national law firm have prepared me well for the diverse challenges I would face if I am fortunate enough to be confirmed.

With respect to the management of lawyers, my experience includes serving as Chief of the Criminal Division in the U.S. Attorney's Office in D.C., which is the largest U.S. Attorney's Office in the country, and now practicing, managing a large office of a major national law firm.

The General Counsel of DHS has a number of critical roles and challenging responsibilities. These include providing legal advice to the Secretary and the senior leadership of the Department, ensuring that the Department's policies and operations comply with constitutional, statutory, and other legal requirements, including the laws that safeguard the fundamental rights and liberties of the American people, and leading and managing over 1,800 lawyers and doing so in a way that promotes morale, high performance, and efficiency. I think those three things go well together.

If I am confirmed, I would be honored to have an opportunity to work with and in support of the tens of thousands of dedicated men and women at DHS who work day in and day out to carry out that vital mission.

One of the things I loved about being an Assistant U.S. Attorney, and I mentioned this to Senator Chiesa when we met last week, I love standing up in court and being able to say, Steve Bunnell on behalf of the United States. I loved having the United States as a client. In fact, I loved it so much that after I left DOJ and when I first went to court as a defense attorney, I stood up and introduced myself on the record as Steve Bunnell on behalf of the United States. The judge was nice about it, but I was actually lucky, I think, not to be fired by my client. [Laughter.]

If I am fortunate enough to be confirmed, one of the things that will mean a lot to me is once again being able to say, accurately, that I am a lawyer for the United States. There is no better client a lawyer can have.

Mr. Chairman, thank you again for this opportunity to appear before you and I would be pleased to answer any questions that you or the Committee has.

Chairman CARPER. Thank you. Thank you so much.

Ms. Spaulding, please. Please introduce your family, if you will.

Ms. SPAULDING. Thank you, Chairman.

Chairman CARPER. And make sure your microphone is on.

TESTIMONY OF SUZANNE E. SPAULDING,[1] NOMINATED TO BE UNDER SECRETARY (FOR NATIONAL PROTECTION AND PROGRAMS), U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. SPAULDING. Thank you. Thank you, Chairman Carper, Ranking Member Coburn, Members of the Committee, and thank you for your gracious welcome of my family.

I am very pleased that they could be here today, my husband, Gary Slaiman; my daughter, Charlotte; my son, Max; one of my seven siblings, Doug Spaulding, who is here; my nephew, Joseph Paradis and his son, Cory Paradis, who is himself an inspiration and a role model with regard to the tremendously positive and upbeat attitude with which he greets each day. I am very grateful to my family for their wonderful support and my children, in particular, who put up with never having a standard routine when they were growing up with two parents working, and so it is really a pleasure to have them here and thank you for welcoming them.

I am honored to be here today with you as the President's nominee to be the Under Secretary for National Protection and Programs Directorate at the Department of Homeland Security.

DHS and NPPD, in particular, is at the forefront of the essential mission of strengthening the security and the resilience of our Nation's critical infrastructure, from water to electricity to communications and the information highway, and even Federal facilities, such as those that distribute Social Security benefits to Americans all across the country.

We focus our efforts on 16 key critical sectors of our economy whose vital services and functions Americans rely upon in their daily lives. Each day, dedicated men and women at NPPD undertake this mission across the country by safeguarding Federal facilities, helping critical infrastructure owners and operators make wise risk management decisions, protecting civilian government networks, and assisting businesses facing cybersecurity threats, and providing leadership on the use of identity management and biometrics to advance our mission.

As Acting Under Secretary of NPPD, and before that as Deputy Under Secretary, I have been privileged to work with outstanding Homeland Security officials inside and outside of government and at both ends of Pennsylvania Avenue who share our commitment to DHS's mission of safeguarding the Nation. We understand that effective homeland security can only be achieved in close collaboration with our partners across the Federal Government, in State, local, Tribal, and Territorial Governments, and in the private sector. I have worked hard to increase the effectiveness of our engagement with these stakeholders, particularly in the private sector, and pledge to continue these efforts, if confirmed.

I also understand that maintaining these vital relationships with the private sector and maintaining the trust of the American public requires a strong emphasis on transparency and privacy protection. Working with our Senior Privacy Officer at NPPD, we endeavor to

[1] The prepared statement of Ms. Spaulding appears in the Appendix on page 106.

ensure that everything we do takes into account the privacy and civil liberties of all Americans.

Another of my priorities since joining DHS has been improving management processes and enhancing efficiencies by better integrating activities across NPPD. These efforts include co-location of our field forces, leveraging experience across our components to better understand and mitigate consequences, and integrating our Operations Centers, the National Cybersecurity Coordination Integration Center (NCCIC) and our National Infrastructure Coordinating Center (NICC). These Operations Centers are good examples of trusted collaboration across government and the private sector.

NPPD cybersecurity innovation has enabled subject matter experts, law enforcement and intelligence professionals, and the private sector representatives to work together on our operations floor to rapidly piece together unfolding threats, get mitigation measures to those who can take action, and strengthening our resilience across critical infrastructures with human knowledge and machine speed. Continuing to build DHS's cyber capabilities will be a top priority if I am confirmed as Under Secretary.

Another area of particular focus has been and will continue to be the Chemical Facility Anti-Terrorism Standards program, which has steadily improved since I joined the Department as Deputy Under Secretary. This important program had suffered from serious management concerns, but over the last 2 years, we implemented significant programmatic and management reforms, and I think it is fair to say that the program has turned a corner. Having said that, there is much to be done and I pledge to continue to place a high priority on making CFATS and effective and efficient program.

None of these mission objectives can be achieved without a capable and committed workforce. I will continue to make it my highest priority to empower the dedicated men and women of NPPD with a clear sense of mission and the tools they need to advance that mission, including strong leadership and capable management.

In addition, we must continue to recruit the best and the brightest to build our capabilities to meet the challenges we face.

Mr. Chairman, if I may, before I close, I would like to echo your condolences for the loved ones of the individuals killed and injured at the shootings at the U.S. Navy Yard on Monday. This tragedy reinforces our commitment at DHS to be vigilant and determined as we continue to work to safeguard Americans and their ways of life.

Thank you very much for the privilege of being here with you today and I look forward to your questions.

Chairman CARPER. Thank you both for excellent statements.

We have been joined by Senator Chiesa. He slipped in. I did not see him. He is our Senator from New Jersey. He is going to be with us for at least another month, and we hope longer. He is just a joy to work with and a real credit to his State, so I am always happy to be with him.

Dr. Coburn, our staffs have been talking for a couple of days now, but he and I spoke today about our concerns about the quality of the background checks that are being performed with respect to

employees of contractors. We have seen with Mr. Snowden, now we have seen most tragically in the last several days situations where contractors had background checks performed, ended up doing work, and creating, as it turns out, in one case a danger to our country, the security of our country at a national level, and then most recently just a real danger to the people who work at the Navy Yard here.

I want to start with you, Ms. Spaulding. Any thoughts you might share with us? Dr. Coburn and I agreed to hold hearings soon to actually look at this process to see how we can do better. And when you have someone who is, in this case, the deceased, the shooter who is deceased who had the kind of troubled past that he had, discharged from the Navy, general discharge, not good, and the kind of arrest record that he had, it is just very troubling.

Any thoughts you have, at least to start off with this? Just give us some thoughts that you have with this issue. We are going to have a full hearing about it, but I would like to start off with that.

Ms. SPAULDING. Thank you, Chairman.

Chairman CARPER. If you would, go ahead. There you go.

Ms. SPAULDING. Thank you, Chairman. This is a very serious concern and I understand——

Chairman CARPER. But before you do, I will ask you three questions. You answered these before, but I am going to ask you again, and then I will recognize you again for your testimony. This is for both of you.

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?

Ms. SPAULDING. No.

Mr. BUNNELL. No.

Chairman CARPER. The record should show that both have said no.

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?

Ms. SPAULDING. No.

Mr. BUNNELL. No.

Chairman CARPER. All right. 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?

Ms. SPAULDING. Yes, I do.

Mr. BUNNELL. I do, too.

Chairman CARPER. OK. Editorial comment I would make. There is a recently released study that indicates again that this Department falls under the purview and oversight of about, I do not know, 70 or 80 different Committees and Subcommittees, which is way too much. We heard time and again, did we not, in the hearing from Secretary Ridge and others that we have to do something about that. So, I realize you just agreed to appear before any Committee or Subcommittee of Congress or reasonably respond. We are going to try to make sure that number is somewhat reduced so you can actually do your job.

OK. Back to the question at hand, if you will, background checks.

Ms. SPAULDING. Yes. Thank you, Chairman.

Chairman CARPER. Contractors.

Ms. SPAULDING. I understand that the President has asked for an interagency review of that process and our Office of Security at the Department of Homeland Security who is responsible for the clearances for our workforce, I am sure we will be a part of that process. And the Federal Protective Service, which is responsible, again, for the security of our Federal facilities all across the country, will be looking at their processes very carefully in the wake of Monday's events, as well.

Chairman CARPER. All right. Mr. Bunnell, any thoughts, please.

Mr. BUNNELL. I do not purport to be an expert on these issues at this point, but I would add that this is an issue that is not limited to DHS. Background checks, obviously, are an issue across the government. I believe the Office of Personnel Management (OPM) plays a major role in managing that, and so I think it is an area where—I am sure the Committee will explore the need for greater consistency and the quality standards across the board.

Chairman CARPER. My colleagues have heard me say more times than they want to remember, one of my guiding principles is do everything well, try to do everything well. I like to say, if everything I do, I know I can do better. I think that is true of all of us. I think that is true of all Federal programs. And this is one area where we have to do better. There are a lot of people depending on us, counting on us.

Mr. Bunnell, if I could, as General Counsel of the Department, if confirmed, your office is going to have a wide array of challenges competing for your attention. Included are threats to critical infrastructure, cyber attacks, airport security, responding to disasters, border security, just to name a few. You will also have the considerable challenge of managing 1,700 lawyers dispersed among the many components of still a fairly new, fairly young and very large Department.

I would like for you to talk with us a little bit today about your past roles at the U.S. Attorney's Office in Washington, the Department of Justice, and also in private practice, just explain for us, if you will, how those different assignments and different posts have helped to prepare you for such a broad mission, and particularly an office with so many attorneys. That is a lot of cats to herd.

Mr. BUNNELL. That is a lot of cats to herd, and lawyers are notoriously catty, or squirrelly, depending on which animal you want to pick.

Chairman CARPER. I have never heard that said about Senators. [Laughter.]

Mr. BUNNELL. You would not hear it from me. [Laughter.]

Senator CARPER. Many of them are lawyers. [Laughter.]

Mr. BUNNELL. As you pointed out, Mr. Chairman, I have had experience in leadership and management roles in different settings and different size sort of groups and organizations. One of the takeaways from those experiences is the kind of basic principles of good leadership and management are applicable in most settings.

So, I think focusing on the mission and being clear in terms of what the purpose of somebody's work is and the values that come with that. So there are certain things which are not negotiable. In-

tegrity, honesty, dedication, you have to have a certain amount of that. That is not negotiable.

And then you have to be clear as a leader in terms of where we are going, and you start with the end and you reverse engineer back. And that, to me, I think, that kind of big picture works with everybody and works in all settings.

And communicating and generating a sense of purpose amongst the people that you are overseeing and leading, making them feel that they are building a cathedral. They are not just cutting stone. And finding ways to communicate that, even with respect to seemingly routine things, because the way things get accomplished is by everybody pulling an oar and then working together as a team. That ethic, that kind of mindset is critical.

My personal approach is very people-focused. When I was Chief of the Fraud and Public Corruption Section in D.C., I came into that job, it was viewed as a place that needed to be sort of energized and more active in terms of outreach. And I sat down and met individually with every person that I was supervising. Actually, I had a little sheet and I went through with them and I asked them, what it is about your job that you find rewarding? What are the things you feel you are good at? Where are the areas that you want to develop as a lawyer? What are the things that are holding you back? What are the frustrations? What can I do as your manager to make you more effective? And that is not only good for morale. You get ideas on how to improve things and you act on it.

And I think I would take that same approach. Obviously, it will be at a higher altitude in a much larger setting, but I would do that with the people that I am going to interact with directly and I would also look for managers and leaders in the sort of chain who understand that and I would make sure they get the training and the guidance to be effective.

Chairman CARPER. All right. Thank you.

A followup question, if I could, and then I am going to yield to Dr. Coburn. Talk to us just a little bit about your goals. You already mentioned this a little bit, but I want to ask you to come back and followup on it a little bit more. Just talk to us about your goals as General Counsel and just mention more fully some of the things you hope to accomplish in this role in the Department. Just complete the picture, if you will.

Mr. BUNNELL. Sure. Well, I mean, obviously, one important goal is to be an effective and valued advisor to the Secretary and the senior leadership, and that is obviously a top priority of the role. Making sure that the Department and its operations comply with the Constitution and the rule of law, that is fundamental to the role of the General Counsel. That has got to be a top priority.

With respect to substantive issues, that is going to be driven by the missions of the organization. I mean, the legal function is in service of the larger missions. So I want to understand how best the legal function can serve those missions.

And echoing something that Dr. Coburn said in his opening statement, I mean, a part of being a public servant is being accountable to the public and I embrace that. I do not view that as a distraction. I view that as inherent in the role. And if you are

in the public service business and you do not want to be held accountable to the people, there is a problem there.

So, one of my goals is to make sure that mindset is instilled into our work and our culture as much as possible within the Office of General Counsel (OGC), and to the extent I can influence larger parts of the Department, because I really think that is fundamental to good, open, transparent government. It is the way the American people get confidence in what we do.

Chairman CARPER. All right. Thank you for those responses. Dr. Coburn.

Senator COBURN. Thank you.

Are both of you aware of the Japanese-initiated management style called Continuous Process Improvement? Have you ever heard of that?

Mr. BUNNELL. I cannot say I have, sir.

Senator COBURN. That is how Toyota became the largest auto business in the world, and I will just share with you a short little vignette. I have been trying to put this into the Department of Defense (DOD) for years, and one segment of the Air Force yesterday that handles about $45 billion a year in expenditures has now instituted that and some things that have come about through that, because the real problem in DHS is morale and morale is a function of management. Actually, it is a sign of poor management. When you have low morale, you have bad management.

This division in the Air Force cut $1.6 billion beyond the sequester this year and is the happiest group in the Defense Department around the country. And the reason they did it is they used smart management techniques.

So, one of the things I would like to hear from each of you, go and find out about this management style that Mr. Toyoda actually implemented, and every major business 25 years ago in this country started doing, and we have very little of it in the Federal Government, but what it does is it creates buy-in from the lowest person on the chain, much as you described. But it is a technique that actually streamlines your organization.

The other benefit, as we all know, is the Pentagon is the only agency that cannot audit itself, and this segment of the Air Force is now auditable, because you cannot manage what you cannot measure.

What I would like is a commitment that you would at least look at that in terms of incorporating it into both managing 1,700 lawyers, but also the thousands of people that are under you, Ms. Spaulding, that are going to require a leadership change. What it does is it does exactly what Steve described in terms of getting buy-in and building a team. So I would love to see you do that.

I am going to spend a few minutes with you, Steve, if I can, just going through a list of questions, and if I do not finish them, I will submit them for the record.

One area in particular is the EB–5 program at Regional Centers are business entities that receive $500,000 contributions from each EB–5 investor, visa applicant, pool them and make investments in businesses that are supposed to create jobs. They are allowing somebody the ability to come in.

In a briefing to my staff, the United States Citizenship and Immigration Services (USCIS) officials told us that they could not shut down a Regional Center based on fraud or national security concerns, that they did not have the ability to do that. That is, even if they were concerned that the Regional Center was committing crimes or helping spies or terrorists get into the country, they could not shut it down.

In August, USCIS leadership told us that they could not shut down an EB–5 Regional Center based on fraud or national security concerns. That is their testimony to my staff.

In your questionnaire, you stated that USCIS had the authority to deny a regional application when a Regional Center applicant fails to demonstrated that the Regional Center will promote economic growth. Are there any other circumstances under which you believe USCIS has the authority to deny a Regional Center application or investor application?

Mr. BUNNELL. Thank you, Dr. Coburn, for that question. I have a general understanding of that program. I know it is a complicated program. It had various iterations over a period of, I believe, about 20 years, and I think it is definitely a program that could benefit from examination.

My understanding of exactly what the legal authorities are to act with respect to fraud and national security risks, which I can certainly see how there could be some, I do not have a specific view at this point. I just have not had an opportunity to have the inside perspective. But you have my commitment that I will look at that. It is obviously a front-burner——

Senator COBURN. I will forward the rest of these questions. It is interesting. Congressional Research Service (CRS) told us that they believe you have the authority to do that now, even though USCIS says they do not, or they have been told they do not. So I will forward you a list of questions for the record, if I may, and have you look at it. It is not fair to pin you down on details of that in this hearing.

Mr. BUNNELL. Yes. Well, I will say that I would welcome an opportunity not to be a naysayer as an attorney and be able to tell people you can do something you thought you could not do.

Senator COBURN. OK. A key provision of the Department of Homeland Security Appropriation Act of 2013 requires the Department to provide this Committee with copies of reports sent to the House and Senate Appropriations Committees. Tom and I actually got that put in so we could actually know what is going on. Oftentimes, we send reports to the Appropriations Committee that are not shared with anybody else, especially the Committee that has the responsibility for it. Yet, some components in DHS have informed my staff that they interpret this section only to cover those reports signed by the Secretary, not the other reports that are going up, excluding any reports issued to the Appropriations Committees by those underneath them, like the Deputy Secretary and heads of the components.

I am especially troubled by that because that was not the intent of Congress. That was not why we put it in. Tom and I are not looking for things to criticize. We are looking for things to fix. And so I would appreciate your response to that, No. 1, and if you do

not feel like responding to it now, a comprehensive response on the record afterward.

Mr. BUNNELL. Well, let me just say that I can certainly appreciate the frustration that situation creates. My sense is that it is related to the problem that I think you both have highlighted, of we have so many different Committees operating at the same time, maybe fighting for their turf more than they are fighting for making DHS as efficient and focused as it can be.

I will certainly take a look at the specific legal issue and also, frankly, look at ways that we can reach accommodations that allow the Committee to get the information that you need to do your job without perhaps antagonizing some other component of the Congress. It is obvious, we are sort of going to be, I think, in the middle a little bit on some of these issues. That is my sense.

But I appreciate what your frustration is and we certainly want to work with you.

Senator COBURN. Well, I would just remind you that this Committee's authority is the broadest in the Congress. This is the Committee on Homeland Security and Government Affairs, and we have broadened that specifically, intentionally, in this Committee in the areas that we have gone.

So you have my commitment, and I think probably I can speak for Tom, we are not going to be asking you questions that are not important to us. We are not going to give you extra work to do. And I have not talked with Tom Carper on this yet, but I think you have way too many Committees demanding information from you, and as far as the Senate, I am going to work, and I hope Tom will work with me, to limit the number of Committees that you have to respond to so that, in fact, you can spend more time managing your Department rather than being on the Hill.

Mr. BUNNELL. We would all appreciate that very much, I am sure.

Chairman CARPER. All right. Thank you. And I look forward very much to working with you on that, Tom.

I am going to go to Senator Johnson——

Senator JOHNSON. Thank you, Mr. Chairman.

Chairman CARPER [continuing]. And then yield to Senator Chiesa.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Let me just give a couple of statistics that Senator Coburn was just talking about. The Aspen Institute, a task force organized by that organization, said that the Department of Defense, which has a budget 10 times the size of the Department of Homeland Security, reports to 36 Committees. The Department of Homeland Security reports to over 100. And in the 112th Congress, there were 289 formal hearings. So I think the first thing we ought to do is look inward and say, what does Congress need to do to become far more effective and efficient in our oversight capability.

Let me start out, first of all, by thanking both of you for being willing to serve. In my short time here in Congress, I am always impressed—I am heartened by the fact I am impressed by the quality of the individuals that are willing to serve their Nation when

I realize there are far more lucrative things that you can be doing with your careers. So, I truly appreciate that.

Ms. Spaulding, you talked about the essential mission of the Department, and I agree with that. In order to actually accomplish that essential mission, the Department also has to be very efficient and effective, which, by and large, is not an attribute that we apply to government. I have certainly learned in my business career that the maximum point of managerial influence is at the point of hiring.

I want to expand a little bit on what Senator Coburn talked about, the oversight capability. I understand how inefficient it is, but also how critical it is. I am a novice when it comes to oversight compared to Dr. Coburn, but one area—and, by the way, from my standpoint, you never know what area you are going to be asked and really asked to look at in terms of oversight.

In my case, with my former Subcommittee, it started with the hearing on Cartagena. As a business person, if we have that kind of problem in my business, I would have gotten to the bottom of that in a week. It has been a year and a half and I still have all kinds of unanswered questions. And as we have gone down that rabbit hole, trying to figure out what happened in Cartagena, and looking at internal investigations and reports of investigations by not only Secret Service, but then the Office of Inspector General (OIG), there are many troubling aspects.

So, I guess, first of all, Mr. Bunnell, I would like to ask you, what do you believe is the role of the Department of Homeland Security General Counsel in relation to the Inspector General?

Mr. BUNNELL. Well, I will start by saying that as a former Federal prosecutor, I spent a lot of time working with Inspector General offices and I understand the importance, not only of their role as sort of one of the—it is kind of a three-legged stool of oversight. There is the direct oversight from the Committee, there is the Government Accountability Office (GAO), and there is the IG. I think those three things are working well together. You get a powerful engine of oversight. And an element of that for the IG is they need to be independent. They need to have credibility. They need to come in and ask hard questions of people that they do not otherwise have to please in their day-to-day lives.

So, the relationship needs to be collaborative and cooperative but, in some ways, arm's length, because there needs to be some independence there. I mean, I would see the General Counsel Office's role really being on the prevention of waste, fraud, and abuse, primarily trying to make sure that your processes and procedures reduce risk. And then if there is a specific instance, an allegation that something, some wrongdoing has occurred, I would assume that would normally go in the first instance to the IG for their investigation and the IG would have to work with the OGC folks and would have to work with the IG to make sure the IG is getting everything they need.

Senator JOHNSON. Let us say there is, hypothetical, a specific investigation being undertaken by the Inspector General. Would the Department of Homeland Security General Counsel have any role in terms of advice in that type of investigation?

Mr. BUNNELL. Well, I think my understanding is that the Inspector General has his own counsel, his or her own counsel, and that person is independent, does not report to the General Counsel. But we would certainly be available, and, I assume, would often be—"we" being the Office of General Counsel, if I am fortunate enough to be confirmed—the expertise of the General Counsel's Office would certainly be available to the IG if they want to understand the way a statute has been interpreted and they need to drill into a specialized area.

Senator JOHNSON. Yes. I am not an attorney, but I think the Inspector General Act of 2008 States that the IG shall obtain legal advice from a counsel either reporting directly to the Inspector General or another Inspector General.

Mr. BUNNELL. Right.

Senator JOHNSON. So, I guess the question I am asking is should the General Counsel of the Department of Homeland Security have any contact with the Inspector General during any particular report, or should it be totally separate?

Mr. BUNNELL. Well, I do not think a total wall of separation would normally be necessary. I think there is a lot of value in making sure that the—the Inspector General has an enormous challenge when they have a specific case. The agents working on that case need to come up to speed on the intricacies of a particular operational area, particular authorities, and if they have questions or they have requests to be briefed on something, I mean, it strikes me as a good idea to have the General Counsel do that so it is done right and it is done quickly so they do not have to spend 6 months learning the area before they can figure out what happened.

Senator JOHNSON. But, again, why would you not have a totally independent counsel to the Inspector General providing that advice as opposed to—again, I am concerned because I think we have seen what I would believe would be improper contact between the Inspector General's Office and the General Counsel of the Department of Homeland Security. I am highly concerned about that and I am trying to figure out what that wall of separation really ought to be to maintain the independence of the Inspector General.

Mr. BUNNELL. Yes. I am obviously not privy to the specifics that are troubling you, and I can certainly imagine situations where the communication would not be appropriate. But just as a broad brush matter, I do not see a problem with having the IG have an opportunity to seek advice from OGC. Otherwise, there is a danger that you then have to essentially replicate the expertise of OGC inside the IG, to a certain extent, and that might not be efficient. So, there is a balance there, as there are in many things. But there certainly should not be an effort by OGC to influence the outcome of and investigation——

Senator JOHNSON. That would be a bright line problem, I mean, improper, if not illegal.

Mr. BUNNELL. Absolutely. The IG is the person who is supposed to find out what the facts are.

Senator JOHNSON. OK. Thank you, Mr. Bunnell.

Senator COBURN. Could I just ask a followup, which begs the question, leadership at the General Counsel's Office ought to give

very strict instruction for cooperation with an IG investigation, would you agree?

Mr. BUNNELL. Absolutely.

Senator COBURN. All right.

Mr. BUNNELL. In fact, lawyers sometimes get a bad rap in terms of being kind of something that slows down, say, the production of documents or providing information. One, they can be proactive in raising that to a top priority for the people in the operational components, and two, sometimes they can help focus in—the goal is not to sort of produce a dump truck of information and then let the IG find the needle in the haystack. Sometimes you can hone in on, what is your priority? Let me get you that first. And that will actually—if you do that in good faith, you facilitate development of the facts, and that is in everyone's interest.

Senator JOHNSON. Can I make one last point?

Chairman CARPER. Sure.

Senator JOHNSON. Again, getting back to the efficiency of oversight, what I have certainly seen during this whole Cartagena investigation and our efforts at oversight is by not having the cooperation of the Department or the Inspector General's Office, it has just forced us to ask for more and more and more documents, things that—I recoil. I mean, when I see the request for information, I do not want to go down that road.

So I guess that would be my point, is if we can really have that cooperative relationship, and again, I have the greatest respect for Senator Carper and Senator Coburn and really for this Committee wanting to be cooperative because we understand that essential mission. So I guess I am just really asking at this moment of hiring to, please, get your commitment to be transparent. Work with us so that we do not have to overburden you with all those types of requests, because that is the natural reaction. When I become suspicious and I am not getting the answers, that is when you start really digging, and I really do not want to go down those roads, quite honestly. Thank you.

Chairman CARPER. Senator Chiesa, you are recognized, please.

OPENING STATEMENT OF SENATOR CHIESA

Senator CHIESA. Thank you, Mr. Chairman, and good morning to both of you and congratulations. I certainly appreciated the chance to meet with you and to discuss your credentials, which I think are, for both of you, outstanding.

And the fact that you are willing to make this commitment to public service is a really great thing, especially when your mission is keeping us safe, because when you boil down your Department's mission, it is keeping the people that live in this country safe. It is an overwhelming task and it seems like we are reminded almost weekly about the different threats that are out there, and we know that through the great efforts of the Department, so many of them get squashed before anything happens.

And I also want to make sure that I thank your families, because I know that any time you enter into these positions, the demands are great, and without the support of your families, you cannot do it. So, thanks to the families, as well, for their commitment and their willingness to let you do this, because I know you have to ask

for permission. I have had to do it throughout my career, so I understand that.

We had a chance to talk about a number of things and I want to start with Ms. Spaulding to talk about cybersecurity. It is something we hear about and something that we know is sort of creeping into our everyday lives. You and I have a chance to discuss a little bit the importance of the Department reaching out to the private sector and having those discussions. Could you talk to the Committee a little bit about your thoughts in interacting with the private sector to make sure that we are doing everything we can as a Department to eliminate or reduce, as best we can, the threats of cybersecurity.

Ms. SPAULDING. Absolutely. Thank you, Senator. And you are absolutely right. As I indicated in my opening statement, there is probably no more important collaboration in cybersecurity than what needs to take place between the government and the private sector. And we work at this every day to improve, continue to improve that relationship and our ability for the government and the private sector to understand the comparative advantages that each of us brings to the table to meet this challenge.

And we do not operate in the same environments. We do not necessarily assess risk and manage risk in the same way. But we do have a shared goal and it is on that basis that we need to continue to come together with a clear sense of those roles and responsibilities based on those comparative advantages, a clearly developed work plan, and a clear understanding of our priorities and our shared goals.

As I indicated, our National Cybersecurity and Communications Integration Center, our operations floor, has seats for cleared private sector representatives who are there, then, to see the information as it comes in, to help us understand that information, help us to quickly develop mitigation measures and get that out much more broadly throughout the critical infrastructure sectors. And that actually has worked very well, but we need to continue to work that.

We need to continue to have these relationships at all levels. So, particularly in the energy sector, we have worked very hard to sustain a working relationship with the Chief Executive Officer (CEO) level. Those individuals are in a position to assess risk across the enterprise, and so it is particularly important that they understand the nature of the threats that we see and that they face and be able to make those resource allocation decisions and ensure that the folks that work for them are making wise decisions.

But also at the Chief Information Security Officer (CISO) and Chief Information Officer levels, very technical ways that we work with them and make sure that we are providing them with, for example, machine readable threat indicators that they are able to very quickly put into their systems, that we are working collaboratively on spurring innovation and developing technology.

So those relationships are critically important and they are a high priority for us.

Senator CHIESA. Good. I know they will continue to be while you are serving.

Mr. Bunnell, you and I had a chance to talk about information sharing. It is something that this Committee is focused on all the time because we know that unless important and carefully vetted information gets where it needs to get, we can have problems in our security.

What I wanted to talk to you about is what role can you play as the General Counsel and the chief advisor to the Secretary in making sure that the Secretary and the other key leaders who have access to the information that we need to stay safe are sharing it in a way that is meaningful and is accomplishing the mission of making sure that information is getting where it needs to get as quickly as possible?

Mr. BUNNELL. Well, I could not agree more that information sharing is one of the sort of core missions of DHS, and one of the reasons it was created was to promote more of that. I remember in the wake of September 11, 2001, one of the roles that I had at DOJ was to try to draft some guidelines to help implement some of the information sharing provisions of the PATRIOT Act, which involved the ability of Federal prosecutors to share grand jury material with the intelligence community or share Title III wiretap information with the intelligence community. You would think that would be simple, but it actually was an enormous process, a lot of stakeholders, a lot of perspectives. So, I think I am sensitive to how what seems easy, share information, can actually be difficult to implement.

I think there is an important role for the lawyers, which is to figure out how to define sharing that everyone is comfortable with and protect information so you are respecting the concerns of whoever collected it, and finding ways to reduce classification on information that is in the national security realm so it can be shared more broadly, and hopefully having clear, widely accepted kind of channels that everybody is comfortable with, because one of the things you see is that some of the turf instincts—which, by the way, come from pride in your work oftentimes, so it is not necessarily an unhealthy thing that people feel a proprietary sense about their sources and methods. I think that is sort of a healthy thing there you do not want to squash. But that sort of pride can sometimes shape somebody's view of what is authorized for sharing.

And so there is a role for the lawyers sometimes to say, no, actually, there is a way to share this information legally, and I use the example of grand jury information. Preexisting documents are not grand jury protected. It is the actions of the grand jury that—I am speaking to you as a former Assistant United States Attorney (AUSA), so you know that Rule 6(e) covers that. So you can find a way to share the content of something that is involved in a grand jury investigation without violating the legal prohibition on sharing grand jury information, and it really requires an attitude that needs to be instilled and sometimes some good lawyering, but sometimes it is just really common sense.

Senator CHIESA. Sure, and I hope that you will do everything you can so that pride never interferes with making sure this information is getting where it needs to get and that you create as clear

of channels as you can while you are there for that information flow to be as accessible to everybody as possible.

So, thank you, and thank you, Mr. Chairman.

Chairman CARPER. You bet.

Let us stick with cybersecurity for a while. I am glad you raised that. Let me just ask, Ms. Spaulding, would you just reflect on what Mr. Bunnell just said and add to, take away, edit, editorial comment. Please.

Ms. SPAULDING. Well, I will not make any editorial comment, on the advice of my counsel. I am a lawyer in recovery, and I am not practicing currently, and I am very respectful of that line.

But I applaud the direction in which Mr. Bunnell is going with his remarks as an advocate for information sharing, and understanding that it is, indeed, at the core of our mission throughout the Department, but particularly in NPPD. That is what we are all about. We are all about getting information out to our stakeholders, again, whether at the State and local, tribal and territorial government level or, most importantly, in the private sector.

And so, we very much appreciate having our counsel close at hand to make sure that we are, again, respecting the privacy and any legal restrictions in place on information sharing, but helping us find a way to accomplish that mission because it is absolutely vitally important. And also at the Federal level, that we exchange information in a very timely way with our Federal inter-agency partners.

So that is absolutely essential for our mission. We, as you know, Senator, would like to see Congress enact some clearer legal authority to clarify the ability for that two-way information exchange between the private sector and the government, and then we would look to our attorneys to make sure that we are implementing it in an appropriate way.

Chairman CARPER. We have three committees in the Senate that share jurisdiction in the cyber world. They include Intelligence, they include Commerce, and this committee, as well.

I think of a comprehensive cyber policy as having at least—being comprised of six discrete pieces. One of those is a critical infrastructure and whoever came up with the idea of the National Institute of Standards and Technology (NIST) being the one to help develop the framework to lead us to best practices within the protection of our critical infrastructure, I think made a very good choice.

Another piece is information sharing, which we are talking about here, between private sector entities and also with us in government, to make sure that there is a good flow of information and that we are incentivizing folks within the private sector—especially those that are dealing with their own controlled critical infrastructure—to follow those best practices and not to feel that they are going to be put out for public ridicule for having screwed up or not provided the very best protection of those elements of the critical infrastructure that they control.

Another piece is the government domain, the .gov domain, what kind of job that we are doing protecting that, not just doing it like taking a photograph once a year and saying OK, how are we doing on this 1 day, but to make sure we are doing continuous monitoring.

Another piece where we want to make sure that DHS, the department that you all hopefully will help lead, that they will have the ability to hire good talent and retain good talent in the cyber world. There is a need for a better job in research and development (R&D). We think we have a role in helping that.

And finally, there is an area that involves data disclosure, not so much our domain in this committee but it is certainly an important element.

Dr. Coburn and I have been working with our staffs and trying to work on—we call it the Federal Information Security Management Act (FISMA)—which deals with the .gov domain. We are trying to figure out for the Department of Homeland Security, what kind of clear statutory authority do you need? Could you, either one of you or both of you—but I will start with you, Ms. Spaulding—just talk about how we can help, at the legislative side, in this area?

Ms. SPAULDING. Mr. Chairman, thank you very much and thanks to both you and Senator Coburn for all of your hard work in trying to help us move this forward in an appropriate way.

You have well articulated key areas where we need some help, and FISMA is one of those. And what that does currently is authorizes, under the guidance and policy direction of the Office of Management and Budget (OMB), DHS to work with the departments and agencies across the Federal Government to assess their networks, assets and systems.

Currently, that assessment takes place every 3 years and produces a fat notebook result, a checklist that leads to report cards that get published in the newspaper for these agencies.

What we are working toward, as you know, is this continuous diagnostics and mitigation, which would be out on the departments' and agencies' systems to assess and diagnose the health of their networks and systems and assets from a cybersecurity perspective and provide them with an analytic result within 1 to 3 days, as opposed to every 3 years. Every 3 days or so that would give them a refreshed view of the security of their network systems and assets.

This would be a tremendous advancement, but the statute provides limited flexibility and without changes we believe we will still require that three-ring binder at the end of the day.

In addition, there are some departments and agencies, well most departments and agencies—and indeed, 23 of the Chief Financial Officer (CFO) Act agencies 23 of the 23—have entered into memorandums of understanding (MOUs) to implement the continuous diagnostics and mitigation (CDM) program. But there are some departments and agencies who have legal constraints that they believe get in the way of allowing DHS to move forward with them on CDM. And so clarification of that authority would be extremely helpful, as well.

Chairman CARPER. I am going to dwell on this for just a moment. There was some discussion on this a week ago during our hearing on the anniversary of September 11, 2001. I want to stay on it just for a little bit.

Unlike the specific authority that defines the Federal Bureau of Investigation (FBI) or the National Security Agency's (NSA) work

in the cyber world, the Department of Homeland Security's authority comes really more through vaguely written laws. Clarifying DHS's existing roles to mitigate against and respond to cyber attacks is something that some of us really hope to address in the legislation that is working its way through here.

Let me just ask, how important is it for Federal agencies like DHS to have clear, explicit lines of statutory authority for its activities?

Ms. SPAULDING. Senator, thank you very much, it is vitally important. Departments and agencies, again in the .gov world, who want to collaborate and participate in these efforts need to be mindful of their legal authorities. They all have wise general counsels who are looking carefully at the authority. And so while we may be able to make a very reasonable argument that the authority is there, they may disagree without clear statutory authority.

The same is true in our interaction with the private sector. Particularly these days private sector general counsels are looking very carefully to ensure that as they share information, collaborate with the government toward these shared goals of cybersecurity that the government is approaching them in ways that are completely consistent with their legal authority. And that is appropriate and that is what we expect.

But as a result, we need to make sure that that legal authority is very clear so they are not reluctant to do what is appropriate and to safeguard our networks and systems.

Chairman CARPER. Thanks. When we come back on the next round, Mr. Bunnell, I am going to explore with you information sharing. How do we incentivize folks to do that? What kind of liability protections are called for? Just be thinking about that. Dr. Coburn.

Senator COBURN. Thank you.

Will you give us a list of those agencies that seem to think they have a statutory problem? Because another way to skin this cat may be changing some of their statutes, rather than change. . . .

One of my big concerns, and I have voiced it in a lot of hearings, is when Homeland Security was created, it was created to be a counterterrorism force. In your testimony, you talked about all-hazards. I will just put this up and you can contest the statement or not. This country does not have enough money for Homeland Security to be an all-hazards agency. There is not enough money. There is not ever going to be enough money.

So my priority, as Ranking Member on this Committee, is to get us back to being very good at what our primary goal is, which is counterterrorism.

I just would wonder about your thoughts on that. We have spent $35 billion on grants to States for things other than counterterrorism, and we do not have any metrics on that. So we do not know if we are any safer or not, because there has been no measurement, no assessment, no accounting for that.

What are your thoughts on my statement about concentrating on counterterrorism first and foremost, rather than being an all-hazards agency? And what the NPPD is really about counterterrorism; correct? I mean, that is what the NP—protectorate—is about.

What are your thoughts on that?

Ms. SPAULDING. So Senator, counterterrorism continues to be one of the Department's absolute highest priorities. And I attend every week an interagency meeting on counterterrorism and engage with our folks who are focused on counterterrorism on a regular basis. And we are very involved with their activities, and that is a key part of NPPD's mission. There is absolutely no question about it.

Having said that, cybersecurity is also a very key part of our mission, and one that is of growing importance.

Senator COBURN. That is counterterrorism.

Ms. SPAULDING. As I indicated in my opening statement, I believe that the overarching mission of NPPD is to strengthen the security and resilience of our Nation's critical infrastructure.

And as I said, that is a focus on making sure that the functions that the American public relies upon are not disrupted by either a terrorist attack, physical sabotage, or by a cyber incident. But understanding how to assess and mitigate those risks requires that we understand the consequences of those disruptions. That is a critical part of that total risk assessment and risk management decisionmaking.

At NPPD, we have been working on that since the inception of the Department. In our Office of Infrastructure Protection (IP) with our critical infrastructure owners and operators to understand the ways in which those functions can be disrupted, the interdependencies across critical infrastructure sectors, the cascading consequences. Those consequences more often will result from a hurricane, a flood, an earthquake, from other natural disasters. And understanding our ability to be in there working with those critical infrastructure owners and operators to understand the impact of those disruptions is a critical part of informing how we understand the impact, potential impact, of cyber incidents, the potential impact of sabotage.

So I really think that a holistic approach to understanding our critical infrastructure sectors and the ways in which we can mitigate those consequences. It is important to address the threats. It is important to understand and address the vulnerabilities. But it is equally important to understand and work on finding ways to mitigate those consequences, which is ultimately what it is all about.

Senator COBURN. I guess where I take exception, I think the likelihood of a counterterrorism event or a cyber event, which is counterterrorism, is much more likely than a natural disaster. One of the reasons we have not seen it is because we have been good and lucky so far.

The other thing I would say, in response to your question, is we are going to understand what is going to be needed to mitigate if we look at the cyber threat and the counterterrorism threat because the results are the same. If you disrupt a pipeline, you disrupt a water supply, if you disrupt electricity transmission. We learn what needs to be done to mitigate if we play those scenarios out.

I believe our concentration ought to be there instead of the other areas.

One question I have, and I have several other questions that I will get for you for the record and give you time to respond to them.

Some duplicative efforts that we are doing that compete with the private sector, and how we handle that and make sure it is there, some of the alert and indicator services offered through the NPPD's Enhanced Security Services (ESS), the Engineering Consulting Service (ECS), and the Industrial Control System Cyber Emergency Response Team (ICS-CERT) parallel services that are already offered in the private sector.

While the Federal Government has this real important role to play in cybersecurity, should we be providing services at taxpayer expense that the private sector is already out there marketing? How do we handle that?

Ms. SPAULDING. That is a very good question, and it is something we are very mindful of. We have no desire to compete with the private sector marketplace. Quite the contrary, our goal is to promote that marketplace and to drive innovation in that marketplace so that is there to meet the needs of the private sector and our critical infrastructure owners and operators.

Having said that, we are also mindful that we have an obligation to ensure that these services and this information is available to businesses of all sizes. The mom and pop shops and the small businesses find very valuable the free vulnerability assessment tools, for example, that the Department can provide.

And so that is what we balance, as we go forward here. We try to lead the marketplace. We try to push the marketplace. If the marketplace catches up and can deliver these goods and services, I completely agree with you, we should get out of that business and move on to the next thing.

Senator COBURN. One final question. There are several open recommendations from the IG on cyber. Two of them date back to 2010. One, establish a consolidated multiple classification level portal that can be accessed by Federal partners that includes real-time incident response related information and reports. That is one, and I know you are working on that. We have had those conversations, so you do not. . . .

Establish a capacity to share real-time Einstein information with Federal agencies to assist them in analysis and mitigation.

Comment on the second one, if you would. I think you agree with those recommendations. We have had conversations about that.

Ms. SPAULDING. We do, indeed, Senator. And we are working hard to close those recommendations, to accomplish the objectives reflected in those recommendations and to close them off. And I believe we have provided to the Committee, to your staff, the status of each of those recommendations. And I share your interest in getting those closed as quickly as possible.

I will say that NPPD has placed a very high priority over the last couple of years on closing open recommendations. We closed 127 recommendations over the last couple of years, but we need to continue to really push that process.

Senator COBURN. Thank you. The rest of my questions I will submit for the record.

Chairman CARPER. OK, thank you.

Mr. Bunnell, I telegraphed my pitch, information sharing liability protection. Any thoughts, please?

Mr. BUNNELL. Well, one sort of—first of all, as we have discussed, it is obviously kind of a core focus of what DHS is all about, is being good at information sharing.

It occurs to me that there is sort of a management phrase that says you have to go slow to go fast, that I think sheds some light on how you go about promoting that.

Chairman CARPER. Here in the Senate of late, we are doing a really good job of going slow. My hope is that some day soon it will be going fast.

Mr. BUNNELL. Well, you have to walk before you can run, right?

What that phrase means to me is that you, in times of crisis, you invest in clarifying roles. You invest in a plan so you are ready to respond. And you invest in relationships whether it is within DHS or whether it is external to DHS—in ways that build trust. So that when something happens, when the fire alarm goes off and people have to go to the incident, they know that their colleagues have their back. They know that everybody is working together as a team and everybody's role is defined.

So just as a kind of broad brush way of thinking about it that, I think, is one of the critical elements. And it is a strategy that the legal function has to be a participant in but by no means is the only participant.

That may have been a little bit more broad than you were interested in, but that is how I—as a sort of approach—that is my mindset coming into it.

Chairman CARPER. That was a little more broad than I had hoped for. Talk to us more specifically, if you will, about the kind of liability protection that might be needed to incent private sector entities that are involved in owning and managing critical infrastructure, and those that are not, to share information. Can you just be more specific, please?

Mr. BUNNELL. I, to a certain extent, would defer to Suzanne.

Chairman CARPER. And I will ask her the same question. This is one of the issues that is dividing. On the Intelligence Committee you have the Chair of the Committee, you have the Ranking Republican. This has been dividing them as they try to find common ground. It has been dividing them for months.

Anything you can do to help us narrow that divide would be great.

Mr. BUNNELL. I am generally aware of things like the SAFETY Act, which are designed to reduce the concerns that the private sector might have about liability associated with the things that we want the private sector to do to make the country safer.

In terms of the specific provisions of that law or other laws that need to be looked at or enhanced, I am not in a position today to get very granular with you other than that I completely agree with you to the extent that the focus is we need to have clear swim lanes, we need to have clear authority. It needs to be simple and clear for it to maximize its effectiveness.

So in that regard, I would echo some of the things that Suzanne said earlier. She has a better sense of the practical reality obviously in the critical infrastructure space.

I do think that—well, the legal issues are—you have to have them, but they are the beginning and not the end of the problem.

Chairman CARPER. Suzanne Spaulding, can you add anything to that?

Ms. SPAULDING. Well, you are absolutely right, Senator. We do need to ensure, with regard to information sharing, that we have very clear authorities. I think that the best protection against liability is to have absolutely clear authority in statute for that information exchange, clearly defined parameters for that exchange, what is appropriate, what is not appropriate, clearly defined privacy protections within that framework.

But it may be that in order to appropriately incentivize that information sharing, that some targeted liability protection may be needed. I think what I would urge is that be very targeted because the system creates liability for good public policy reasons, generally. And so any liability protection that goes into place should be very targeted.

But the information sharing, as we have talked about today, is absolutely vital. And so we very much appreciate your work, Mr. Chairman, and the Committee's work to find a way forward on this.

Chairman CARPER. Thank you.

If you all are confirmed, and I hope you will be, we will talk about this some more, I am sure.

I want to come back to the issue of morale. Every Wednesday morning there is a bipartisan breakfast that maybe—I do not know—10 or 20 Senators participate in, Democrat and Republican. It is called a prayer breakfast. There is some prayer and there is some scripture, people of different faiths. But there is just a lot of personal sharing. It is a good way for us to get to know one another better.

I usually do not get to go because it is from 8 to 9, and I am usually on a train. I go back and forth almost every night to Delaware and it is hard for my train to get here before 8:45 unless I get up at about 3 in the morning and I do not do that often.

But anyway, they asked me to speak this morning. It was a real honor for me to share with my colleagues.

One of the things I talked about was an NPR study that came out about a year ago. They had done a survey around the world—someone, not NPR, but someone else. They were just reporting on it on NPR. The question that was asked in the survey was what do people like about their job. What is it that makes people like their work?

People had all different kinds of answers, as you might imagine. Some folks said they liked getting paid. Some folks said they liked getting to go on a vacation. Some folks like the pension. Some folks said they were happy they had health care. Some people said they liked the people they worked with. Others said they liked the environment in which they work.

But do you know what most people said? Most people said the thing that caused joy or satisfaction in their work, for most of them, was that they felt like the work they were doing was important and they felt like they were making progress.

My admonition to my colleagues this morning was that the work that we are doing here is very important. We are not making the kind of progress that we need to make.

I love to ask people who have been married a long time the secret to being married a long time. I get great answers, I get hilarious answers, and I get some very poignant answers, as well. Among the best answers I have ever gotten are the two C's, communicate and compromise.

That is not only the secret for a long union between two people, it is also the secret to a vibrant democracy.

Now, that is a long lead-in to the morale challenges that we face at the Department of Homeland Security. Dr. Coburn talked a bit about management as part of the solution. That is part of it. A big part of it is leadership. Frankly, we do not have any Senate-confirmed leadership at the top of the Department, as you know.

Secretary Janet Napolitano has run off to California to run the University of California system. It is a great job, she will do well. She did a very fine job, along with Jane Holl Lute, in running this Department for the last 4 years. A lot of progress—GAO reports a lot of progress in the terms of the high-risk list, a lot of things have been addressed. It is an auditable—the finances are auditable now, and my hope is we will get an unqualified audit within the year. So real progress is being made.

In terms of morale for employees, I think it is right at the bottom.

So one of the things I think we need to do is confirm the leadership through good people that the President has nominated. He needs to nominate somebody to be secretary and he has not done that yet. He has nominated someone, I think a very good person, to be the deputy secretary.

Senator Johnson was talking about the IG's office in the Department of Homeland Security. We have not had a confirmed IG for over 2 years. We have had one nominated, that nomination was stalled by someone in this Committee, and then that person finally gave up and the Administration gave up and that nomination was withdrawn. Maybe for good reasons. I am not here to judge the quality of the candidate.

Another person was vetted for the position of OIG head, a person from California, apparently a good person. They got near the end of the vetting process and said I do not think I want to do that, I do not want to get into that mess in Washington. Why would I move my family to Washington to put up with all of this? Don't any of you get cold feet here. That person said enough, I do not think I want to do that.

So now we have not had a confirmed Inspector General in this department for 2 years. The one who is Acting, if you will, as the Inspector General is under investigation by a Subcommittee of this Committee. They are allegedly doing their own investigation of the President's nominee for Deputy Secretary of the Department of Homeland Security. I do not know if you know him at all, Alejandro Mayorkas, Ms. Spaulding.

But some of our colleagues are wrestling with how to proceed on the nomination, whether to proceed or not. The last inspector gen-

eral who was confirmed by the Senate actually sent a very strong letter in support of Alejandro Mayorkas.

If you know him at all, if you can share any insights into his abilities, his work ethic, his integrity, that would be great.

Ms. SPAULDING. Thank you for that opportunity, Mr. Chairman.

I did not know Alejandro Mayorkas before he was nominated to this position. But as part of his preparation we, at NPPD, had the privilege to bring him up to speed on our issues. And as you know, they are very complex issues. There is a lot of activity underway in NPPD. We had a number of briefing sessions with him.

I found him to be incredibly engaged, clearly passionate about this mission area, very smart, a very quick study, and a very decent individual. I was very optimistic about the kind of leadership that Alejandro would bring to the Deputy Secretary position.

I am grateful for the work that you are doing to try to move forward on his confirmation and I urge the Committee to do that.

Chairman CARPER. I said to some of my colleagues, here we are a week after September 11, 2001. We are in the midst of this crisis at this time with Syria, we are going to start firing rockets at them. We have this terrible tragedy two miles away at the Navy Yard. We do not have a confirmed Secretary, we do not have a confirmed Deputy Secretary. It is not a good situation.

I feel a sense of urgency and it is just important that all of us feel that sense of urgency.

I want to ask, to me one of the elements affecting workforce morale, you have these 22 disparate agencies we have kind of glommed together to create the Department of Homeland Security less than a decade ago. They are, for the most part, still scattered to the winds. On Monday, on my way into D.C. from Delaware the Senate was shut down, the Capitol was shut down—at least on our side—for a while. So as we drove in—normally I take the train but as we drove in from Southern Delaware I said the Capitol is shut down for a while, why don't we go to the Department of Homeland Security and actually get briefed there.

As you know, the agencies are scattered throughout Washington. But most of the folks are, a big part of the folks are—including the Secretary's office and some of the senior leadership, it is like a rabbit's warren to get from one place to the other.

If you get confirmed, Mr. Bunnell, you might want to get a GPS or something. It will help you navigate through that system, because it is not easy.

But there is an effort to try to create a campus at St. Elizabeth's and to actually, over time, bring everybody in. How important is that, in terms of enhancing morale? And if we want to really be one DHS, how important is that to getting us to that spot? We have the Coast Guard there. They just had the ribbon-cutting a month or so ago. They are there. It is a beautiful start.

Your thoughts on that?

Ms. SPAULDING. Mr. Chairman, NPPD alone is in, I believe, 10 different buildings just in the National Capital Region (NCR), which presents some significant challenges. As I indicated, one of my priorities is integrating our activities across NPPD, helping all of our components and the folks that work in NPPD understand how their missions relate, how they can leverage each other's re-

sources and expertise in these difficult budget times. We have to do that. That is a critical part of our efficiencies. And it is made more difficult and more challenging by being physically spread out around the region.

So being able to come together, as much of DHS as could fit within that St. Elizabeth's compound, would I think make a very significant difference and be of significant help in bringing this still very young department together.

Chairman CARPER. Mr. Bunnell, any thoughts on this?

And also, the other question I am going to ask you, is to talk a little bit about your own leadership style and how that might be seen as affecting—hopefully positively—the morale of the folks that you would be leading. Go ahead, please.

Mr. BUNNELL. Sure. Let me just first put in a quick plug for Ali Mayorkas. I know you asked about it before.

Ali used to be a law partner of mine.

Chairman CARPER. Is that right? Oh, that is right.

Mr. BUNNELL. I feel like—I will say, when people ask me why do you want to do this job, one of the reasons is there are people like Ali Mayorkas at the Homeland Security Department, and I would love to work with people like that.

I think he is as good as it gets, in terms of public servants. He had an outstanding reputation when he was the U.S. Attorney in L.A. He was a career guy that was made the U.S. Attorney. That does not happen very often.

In fact, my introducer, Ken Wainstein, who does not really have a dog in this fight, reminds me that he actually has written a letter in support of Ali, and knows Ali. I do not know if you have anything you would like to say on the record, since we have been invited to put in a plug for Ali.

He would be a wonderful Deputy Secretary.

Chairman CARPER. Mr. Wainstein, I did not realize that. Thank you. We have received a lot of letters.

Mr. WAINSTEIN. Thank you, Mr. Chairman. I appreciate the opportunity.

I was a law partner with Ali as well, at O'Melveny and Myers. But I knew of him as the U.S. Attorney.

As Steve said, some of the things that I have described about Steve, that made me so fond and have such admiration for Steve, apply to Ali as well.

Long-time career guy. He was in the trenches in the U.S. Attorney's Office and rose up to become the U.S. Attorney. He looks at an issue apolitically. He looks at what is best for the mission and what is best for his agency. He did that in the U.S. Attorney's Office. He jumped into what is a very difficult job at the beginning of this Administration and has done a fabulous job with it, hence the promotion or hopeful promotion. But he has done it in a way that showed that he has really put the mission and management above anything else.

That is the kind of person you want at DHS. I am disappointed that there has been a delay, but I know Ali and I know that this issue is going to go away and he is going to do a bang-up job.

Chairman CARPER. From your lips to God's ears. That would be good. Thank you all for saying that.

Let me turn to management, your own leadership style and how it might enhance morale and, frankly, be an example to other leaders in the department, please. Ms. Spaulding.

Mr. BUNNELL. Was that to me?

Chairman CARPER. Excuse me, go ahead, and then I will come back to Mr. Bunnell.

Mr. BUNNELL. I am sorry.

Ms. SPAULDING. Mr. Chairman, thank you for your emphasis on this. This employee morale has been an issue that I have spent a great deal of time and focus, effort and energy on, as has the team around me within NPPD.

The employee survey results from 2010 were being analyzed by the team when I came on board in 2011. The results had just come out. They were already hard at work understanding those results, trying to make sure they understood what the workforce was trying to tell them, and implement an action plan to address those concerns.

So for example, a clear reflection of concern about the quality of leadership, particularly at the supervisor and secondary supervisor level within NPPD. And so we have beefed up our training of our supervisors and came up with a leadership and a performance culture training class which I have been fortunate enough to participate in. I go in the morning, I talk with the students in the class, our supervisors that are there, about my leadership goals and management objectives, and listen to their concerns. I come back at the end of 2 days to hear the results of what they have gotten out of the class. It is a terrific step forward for us in making sure that we have equipped our supervisors who have stepped up to this responsibility with the tools they need to do a good job.

As I tell them, I think we often in Washington have an image of leadership that is an organization with the leader at the top of the pyramid and everybody in the organization is working to support that leader. I realized years ago that that was a fundamental misconception and we need to flip that pyramid on its head.

As leaders, we need to remember that we are there to empower and enable the individuals who are out there getting our mission done. I am a firm believer that it is our responsibility to do everything that we can to make sure, as I said, that they have a clear sense of mission. I totally agree with you that these people who have chosen public service, which I think is so honorable, did so because they wanted to make a difference.

I feel a tremendous obligation to make sure that I do everything that I can so that at the end of the day, when they leave work, they feel as though they are making progress, that they are making a difference, that they are part of a team and an effort and a mission that is bigger than themselves and that matters.

So I could not agree more.

Chairman CARPER. That is great.

Ms. SPAULDING. It is absolutely important.

I would just add, just to clarify the record, one of the areas where leadership has been particularly important, is with our CFATS program, our Chemical Facility Anti-Terrorism Standards program, where we brought on new leadership just before I came onboard.

The current leadership there, David Wulf, has really done an outstanding job.

The statistics, which I want to clarify for the record, on the progress they have made over the last 2 years, they have actually authorized seven——

Chairman CARPER. You are anticipating my next question and my last question perfectly. So just go right ahead, and then I will come back to Mr. Bunnell. We are going to close with CFATS.

Ms. SPAULDING. I appreciate your indulgence because the team has worked so hard to make this kind of progress, I think it is important to get into the record.

They have authorized over 700 site security plans of chemical facilities across the country. They have inspected over 400, and they have approved nearly 300 site security plans for our facilities across the country.

They have made remarkable progress in streamlining and expediting that process without sacrificing the national security imperative.

Having said that, we know that we need to do even better because the bulk of our work needs to be done at tiers three and four and, while we have nearly completed the highest risk tiers, we have a lot still to get through and we are working hard to come up with processes that will allow us to get through those much more quickly.

And we are working closely with our private sector stakeholders on that effort.

Thank you.

Chairman CARPER. I said earlier, if it is not perfect, make it better. Thank you for making it better, and for everybody that has been a part of that.

Mr. Bunnell, leadership? Very brief on this, very brief.

Mr. BUNNELL. Sure.

Chairman CARPER. Leadership and morale.

Mr. BUNNELL. I would just commend you for your role in trying to find a campus where everybody can get together. One of the things that I have found that is very helpful, in terms of promoting morale, and I think it is part of my management style, is management by walking around.

And right now——

Chairman CARPER. I try to do that myself, always have.

Mr. BUNNELL. Then you know how valuable and effective it can be.

Right now, I think DHS is in a situation where, at least for the leadership, it is management by driving around or flying around. And that is a level of challenge that we do not need on top of all of the challenges, the history and size and all of the other things.

So I think once we get everybody in the same place, that will help a lot. Because it is those small, casual interactions that build morale as much as the big speeches. So I commend you for that.

In terms of things that I will do within OGC, I do not know specifically what, if any, morale issues there are in OGC as opposed to the Department writ large, but I will certainly be focused on it because morale is not just about feeling good. It is about doing your job well, performing well, being efficient. That is what makes peo-

ple feel good about their jobs. And that happens to be good for the American taxpayer, too.

Chairman CARPER. OK. That is a good note to close on.

We have some other questions for the record. The hearing record will remain open until noon tomorrow for the submission of statements and questions for the record. I would just ask that you respond promptly to those.

My hope is to move these nominations quickly. That is, I think, a goal that is shared by Dr. Coburn.

Both—Mr. Bunnell, both you and Ms. Spaulding, have filed responses to your respective biographical and financial questionnaires. You have answered pre-hearing questions submitted by the Committee, had your financial statements reviewed by the Office of Government Ethics. Without objection, this information will be made a part of the hearing record, with the exception of the financial data which are on file and available for public inspection in the Committee offices.

With that having been said, we thank you both for your presence today, your preparation for this hearing, for your answers, and for the answers you will provide to subsequent questions that are asked.

Again, to all the family members that are here, moms, dads, spouses, children, other friends and admirers, thank you for being here to have their back during the course of what I think has been a very good hearing.

Mr. Wainstein, especially thank you for your comments on Ali Mayorkas and actually for, Steve, for yours and Suzanne, too. We need to provide leadership for this department and we need to provide it soon. This is a shared responsibility. The White House, the President needs to do his job, we need to do ours.

And on that, I will say class dismissed, the Committee is adjourned.

Thank you.

[Whereupon, at 11:31 a.m., the Committee was adjourned.]

APPENDIX

Opening Statement of Chairman Tom Carper
Nominations of Stevan E. Bunnell to General Counsel, U.S. Department of Homeland Security, and Suzanne E. Spaulding to Under Secretary for National Protection Programs, U.S. Department of Homeland Security
September 18, 2013

As prepared for delivery:

Before we get started, I would just like to extend my deepest sympathies to the friends and families of those we lost during the shooting at the the Navy Yard on Monday. I would also like to commend the brave law enforcement officials and other first responders who rushed to the scene of this terrible tragedy.

It is my hope that we can learn as much as possible from this incident so we can prevent these types of tragedies in the future. I know the Department of Homeland Security will be doing its part to learn from this incident and keep Americans safe.

Today we meet to consider the nominations of Stevan Bunnell, President Obama's choice to serve as General Counsel of the Department of Homeland Security and Suzanne Spaulding, the President's nominee to be Under Secretary for the National Protection and Programs Directorate. These positions are extremely important to the Department and to the security of our nation.

The National Protection and Programs Directorate, for example, is responsible for securing our nation's critical infrastructure from cyber attacks. The General Counsel serves as the Secretary's chief legal advisor and ensures that the Department's activities are consistent with the Constitution and the laws we make here in Congress.

I know my colleagues and I on the Committee are very pleased to see the President put forth nominees to fill the leadership vacancies in these critical components. The Administration has made some recent progress towards filling the number of vacancies at the Department. From what I understand, nominations are pending for four of the eight senate-confirmed vacancies at DHS. Of course, that still leaves four positions without even a name put forward – including the Secretary and Inspector General. It is imperative that we get all of these vacancies filled as quickly as possible.

As I have said before, the confirmation process is a shared responsibility. The Administration has a responsibility to provide us names of excellent people – honorable, hardworking and capable people – who can provide strong leadership not just at the Department of Homeland Security, but across government.

And my colleagues and I here in the Senate have an obligation to exercise our "advice and consent" responsibilities in a judicious but timely manner. If the nominee is qualified, we need to move him or her quickly. This morning, we have before us two people who I believe are very well-qualified.

Stevan Bunnell has over 25 years of experience practicing law. For seventeen of those years, he served in positions of increasing responsibility as a prosecutor and supervisor at the Department of Justice, including as Chief of the Fraud and Public Corruption Section and Chief of the Criminal Division in the U.S. Attorney's Office in Washington D.C.

In addition to working with a variety of law enforcement agencies on complex criminal cases, it's my understanding that Mr. Bunnell also worked closely on national security issues with someone we are all very familiar with – Michael Chertoff – then an Assistant Attorney General at the Department of Justice. Later, Mr. Bunnell left the government for private practice. He is currently serving as the managing partner of the law firm O'Melveny and Myers in Washington D.C.

Our second nominee is Suzanne Spaulding. She comes to us with a rich background in both government service and work in the private sector. She is currently serving as the Acting Under Secretary for the National Protection and Programs Directorate. Before that, she served as a Deputy Under Secretary in the directorate.

Ms. Spaulding's distinguished career has also included positions as the General Counsel for the Senate Select Committee on Intelligence, Staff Director for the House Permanent Select Committee on Intelligence, and as an attorney for the CIA. She also has several years of experience in private practice. In her current post at the Department of Homeland Security, she has brought a direct and engaged management approach to some of the Department's most important missions.

Over the course of their respective careers both of our nominees have shown themselves to be natural leaders. In addition, both have become widely respected by their peers for their intellect, professionalism, and integrity. I believe these are the types of qualities we want to see in our government leaders. I'd like to ask for unanimous consent to enter into the record all of the letters of support we received that speak to the great attributes of our nominees.

To conclude, I would just like to thank both of our nominees for their willingness to serve our nation. I would also like to thank their families for sharing them with us. We know that public service it is not always easy and that a lot of sacrifices must be made, so we thank both you and your families for your commitment to our nation and for being here today.

###

Opening Statement for Sen. Tom Coburn
Nominations of Stevan E. Bunnell to be General Counsel, U.S. Department of Homeland Security, and Suzanne E. Spaulding to be Under Secretary for National Protection and Programs Directorate, U.S. Department of Homeland Security
September 18, 2013

Good morning. Thank you for being here today.

Leadership vacancies are one of the biggest challenges facing the Department of Homeland Security. Last week, this Committee held a hearing looking at lessons learned and challenges facing the Department of Homeland Security.

We heard from former Secretary Ridge and other former senior officials about the many challenges facing DHS—from questions about Congressional oversight to mission creep and successful integration of the Department and its components.

A clear take-away was that it will require real leadership to address these problems and create a well-functioning Department for the next 10 years.

One of the biggest challenges facing the Department is its many leadership vacancies. According to information provided by the Department and our analysis, there are currently 15 senior leadership positions unfilled at DHS, 8 of which are Senate confirmed and 7 that do not require Senate confirmation.

If DHS is going to address it's many challenges—and become a well-functioning Department—it will require strong and effective leadership atop the Department and at each component, office, and directorate.

I am hopeful that the two nominees under consideration today will earn the Committee's support and be confirmed.

Each of you has an impressive resume, and experiences and knowledge that make you well-qualified for the positions to which you have been nominated. Ms. Spaulding, I have appreciated our meetings and candid conversations about the challenges at NPPD. Mr. Bunnell, I have reviewed your background and your questionnaires, and understand that you are well-qualified for the General Counsel's position.

But by earning the trust and support of our Committee, we ask for your word and assurance that we will be partners in working together to fix the Department.

Conducting oversight and asking questions on the American people's behalf is one of our committee's main responsibilities. Unfortunately, too often DHS doesn't cooperate with our oversight requests, and has undermined what could be a collaborative process to identify and fix problems.

For example, when the Permanent Subcommittee on Investigations was doing our bipartisan investigation into the fusion center program, DHS seemed to use every tool they could—including making weak legal arguments—to drag out the process and undermine the oversight process.

The result was a significant in our investigation, which ultimately found significant problems in that program.

And that was a "lose-lose" for DHS, the Congress, and frankly the American people who are paying for these programs.

Instead of spending those two years fixing the problem—and figuring out how DHS's intelligence program could yield better value for the American taxpayer—we were stuck in absurd legal debates over document production.

In other cases, I asked basic questions and didn't receive straight answers from the Department. For example, during the Immigration Reform debate, I asked Sec. Napolitano whether she could share with me her sector-by-sector border security plan and provide a "Congressionally-Mandated Border Security Status Report." The initial report was due to Congress in February 2012.

However, I didn't get a plan or the report. And what little information I did get was not helpful.

So our committee and the Senate had to vote on the Immigration Reform bill without a clear understanding of the Department's border security strategy.

Today, I ask you to partners with our Committee and to pledge to be cooperative with our Committee and the Congress in the oversight process.

Mr. Bunnell, as the General Counsel, you will have the responsibility of overseeing how the Department and its components respond to Congressional oversight requests. I ask you to commit today to being supportive and cooperative of these requests.

Ms. Spaulding, as the Under Secretary for NPPD, you will be overseeing a Directorate with a troubled track record. As you know, this Committee and Congress have had serious questions about some of the key initiatives that your Directorate oversees—such as the CFATS program for

Chemical Facility Security and cyber security. I ask you to be candid with our committee and forthcoming when we ask you questions.

Working together—through this oversight process—I'm certain we can strengthen the Department.

I plan to discuss some specific policy issues this morning.

But I will close for now by thanking you for being here today and for being willing to serve. I look forward to hearing your testimony and hopefully working with you to help fix the Department over the next three years.

Opening Statement of Sen. Tim Kaine
Introducing Suzanne E. Spaulding
Nominee to be Under Secretary, U.S. Department of Homeland Security
September 18, 2013

Thank you Mr. Chairman, and Ranking Member Coburn and committee members; it is a treat. This is a real example of the best and brightest being here for Suzanne, and I think we often have hearings where it's about the best and brightest, but I don't remember doing one where I thought it was the best and brightest who was so particularly suited for this particular position.

To begin, as my friend Mark mentioned, her family has a great family career in public service, both in civilian public service and also service in the military: her parents, her brother, her sister and Suzanne. We may not do all we need to do to honor the service of those who serve the country in both a military and civilian capacity; we learned to our horror two days ago that there are sacrifices, including sacrifices that you don't expect to happen, but this family has sacrificed for public service in some really notable ways and I begin there.

And second, Mark talked a bit about her background, you know Suzanne has worked for twenty five years in this field of trying to advocate for the nation's security, in the private sector and in the public sector, in the public sector at the federal level and at the state level, at the federal level in the Executive and in the Legislative, and in the Legislative for Democrats and Republicans, and for Senate and House. She's touched this issue from virtually every angle, and made it her life's work and her life's passion.

And in serving in this acting capacity, she has earned the confidence of this administration, and she's also earned the confidence of two previous DHS Secretaries, Secretaries Chertoff and Ridge, who have strongly weighed in on her behalf, and I think all that speaks very well of her nomination and urge it to be considered favorably and promptly.

Opening Statement of Sen. Mark Warner
Introducing Suzanne E. Spaulding
Nominee to be Under Secretary, U.S. Department of Homeland Security
September 18, 2013

I am honored to be here today to introduce Suzanne Spaulding as the President's nominee for Under Secretary of the National Protection and Programs Directorate at the Department of Homeland Security.

As a friend of Suzanne's for over 30 years, I can personally attest that there are few people who possess the kind of intellect, experience, temperament and passion for the Department's mission as does Suzanne.

I urge this Committee's swift approval of her nomination.

I would also like to acknowledge the public service of Suzanne's mother and father, both of whom served this Nation in the Marines, as did her brother Doug, who is here today.

I have benefited from Suzanne's advice on national security and homeland security matters over the years. Whether through her service on Capitol Hill, at the Central Intelligence Agency, in the private sector, or at DHS, Suzanne has dedicated her career to making this Nation safe and secure.

When I became Governor of Virginia in 2002, I appointed Suzanne to the Secure Commonwealth Panel to advise me and the Commonwealth on safety and security matters.

However, Suzanne's career has been bipartisan. She has worked across the aisle on many occasions. For instance, she served as Legislative Director to Senator Arlen Specter and worked with former Virginia Governor Jim Gilmore in his capacity as chair of a Commission to assess the nation's capabilities for responding to a catastrophic terrorist attack.

Not only does Suzanne have national and homeland security experience and expertise, she also brings unique perspectives from the private sector and understands the critical role State and local governments play in homeland security.

As my experience in business has helped inform the choices I make in government, so too will it help Suzanne as she spearheads DHS's engagement with the private sector on cybersecurity and critical infrastructure protection.

Cyber threats require a unique public-private partnership and there is no one better than Suzanne to forge that relationship. Her years as counsel to many critical infrastructure owners and operators and work with national organizations like the Business Roundtable, gives her incredible insight into the needs and innovation of the private sector.

The myriad threats facing the Nation, particularly in cyberspace, keep us up at night. With talented public servants like Suzanne protecting the Nation, we can rest a little easier.

Statement of Kenneth L. Wainstein
Partner, Cadwalader, Wickersham & Taft

Before the

Senate Committee on Homeland Security and Governmental Affairs

September 18, 2013

Chairman Carper, Ranking Member Coburn and Members of the Committee, I appreciate the opportunity to appear before the Committee today with my friend, Steve Bunnell, and his family as the Committee considers his nomination as General Counsel of the Department of Homeland Security. I consider it a distinct honor to introduce Steve, given both the critical importance of that position and the sterling character of the nominee.

I am currently a partner at the law firm of Cadwalader, Wickersham & Taft. Prior to entering private practice in early 2009, I served for over twenty years as a lawyer in the federal government – first as a career federal prosecutor, then as FBI General Counsel and Chief-of-Staff, United States Attorney and Assistant Attorney General for National Security, and finally as Homeland Security Advisor to President Bush. In each of those positions, I had the opportunity to work closely with Steve. Given this history, I feel particularly well-equipped to speak to his suitability for the DHS General Counsel position.

Before providing my personal perspective, I would like to take a moment to go through Steve's resume and his objective qualifications for the job. Steve graduated Phi Beta Kappa from Yale University and then from Stanford Law School, where he served as senior editor on the law review. He clerked for highly-respected Judge Silberman on the D.C. Circuit Court of Appeals, and then spent some time in a law firm before serving for five years as one of the strongest line prosecutors in the United States Attorney's Office in Washington, D.C. From

there, Steve transferred to Department of Justice headquarters at "Main Justice" where he handled some of the Department's most important and sensitive public corruption prosecutions before being asked to serve as counsel to the Assistant Attorneys General for the Criminal Division for both the Clinton and the George W. Bush administrations. He ended up his government career back at the D.C. United States Attorney's Office, serving first as Chief of the Fraud and Public Corruption Section and then as Chief of the Criminal Division. In the latter position, Steve oversaw the establishment of a new National Security Section responsible for the prosecution of international terrorism, espionage and other national security crimes and he represented the Office in the Department's policy discussions about the myriad national security issues that arose in the years after 9/11.

Those are Steve's credentials on paper. Let me now explain why those credentials and Steve's character add up to the ideal nominee for the DHS General Counsel position. I base this opinion both on my understanding of the demands of that job – derived from my experience in comparable government positions – and on my close working relationship and friendship with Steve over the past 21 years, a friendship that has given me a very clear understanding of the man and his character.

Steve is a natural choice for the General Counsel position for several reasons. First, he is quite simply an excellent lawyer, one of the very best I have ever worked with. His analytical skills and judgment are exceptional, having been honed through years of wrestling with tough issues of law and fairness as a line prosecutor and equally tough issues of national security policy as a high-level Justice Department official. Steve's balanced, thoughtful approach to difficult and controversial issues makes him the ideal counsel to an agency that regularly confronts such

issues, and is the reason why Steve has always been the first person I seek out whenever I need sound and honest advice in a tough situation.

Besides being a tremendous legal talent, Steve has exceptional leadership skills – skills that will be absolutely critical for a General Counsel who is responsible for both managing an extended group of DHS lawyers across a wide spectrum of agencies as well as representing the Department with strength and credibility in the inter-agency process. Steve's leadership qualities have stood out throughout his career – from his service as Chief of the Criminal Division when we were together at the United States Attorney's Office to his successful tenure as Managing Partner of O'Melveny's D.C. office over the past few years. At every step of his career, Steve has shown himself to be a natural leader who sets the example for the rest of his colleagues.

Steve has also proven himself a true government professional in the best sense of the word. From his earliest years as a line prosecutor, Steve has established a reputation as a completely apolitical straight-shooter and as someone who always subordinates political interests to the mission and to the needs of his agency and his country – a reputation that is reflected in the glowing letters of support this Committee has received from persons across the political spectrum. This apolitical approach is critical in all aspects of government, but particularly in a law enforcement and national security agency like DHS whose effectiveness is so dependent on having the trust of Congress and the American people.

Lastly, and most importantly, Steve is a man of honor who has the personal character one would want in such an important and sensitive position. Steve is universally respected and admired by all who have ever worked with him – from the Attorneys General and Deputy Attorneys General of both parties who have relied on his counsel to the O'Melveny associates who have flourished under his inclusive management style. Steve has earned that admiration in

part by his smarts and hard work, but also because he has had a career that exemplifies the qualities of integrity, decency and fidelity to public service. His willingness to step out of a highly successful law firm partnership and into the DHS counsel position is just the most recent example of Steve's selflessness and sense of duty.

In sum, I cannot think of a better person to assume this important role at this critical juncture of our history. I am confident that Steve will serve with honor and distinction and that the people of our country will be more secure both in their safety and in their civil liberties thanks to Steve's service as General Counsel of the Department of Homeland Security. I therefore give Steve my unqualified recommendation, and urge the Committee to endorse him unanimously.

Statement of Stevan E. Bunnell

Nominee for General Counsel,
U.S. Department of Homeland Security

Before the

Senate Committee on Homeland Security and Governmental Affairs

September 18, 2013

* * *

Thank you, Mr. Chairman, Ranking Member Coburn, and Members of the Committee. Let me also thank my good friend Ken Wainstein for his very kind introduction today and his support throughout the confirmation process.

It is an honor for me to be here today as the nominee to be General Counsel of the Department of Homeland Security. I thank the President for his confidence in me, and I thank the Committee for moving forward so expeditiously on my nomination.

I would also like to thank and recognize the members of my family who are here today: My wonderful wife, Laura, who has always been so supportive of my passion for public service, despite the many sacrifices it imposes on her and on her own successful law practice. I don't know how she does it all, but I do know that she is truly my better half.

We have two sons -- Philip, who is in college in California, and could not be here today, and Daniel, who is a senior in high school, and is here today. Philip and Daniel are not only my pride and joy, they are also a reminder to me that the work being done on homeland security today is not just about keeping us safe in the present, it is about building a foundation for a safe,

secure, and resilient future for the next generation, and making sure that future generations enjoy not only physical security, but also the fundamental rights and freedoms that we all hold dear.

I am grateful that my parents, Fred and Alice Bunnell, are here today. Both of my parents are retired teachers. They instilled in me and my sisters a strong ethic of service, of giving back. They continue to be an inspiration to me.

I would also like to thank my two sisters, Becky, who works for the Centers for Disease Control in Atlanta (and is here today), and Ann, who is a social worker in Chicago. I owe them special thanks for helping me, as only siblings can, to learn at a young age how to share toys, share chores, and work together with people I do not command or control. Those sibling experiences provided a foundation for skills that have served me well in life so far, and are skills I'm sure I will continue to rely on, if I am confirmed.

Finally, I would like to thank my wife's parents, Rod and Carla Hills, for being here today, and for being role models not just for me, but for anyone who aspires to serve our country with distinction and integrity at the highest levels of government.

I'm excited about the possibility of returning to public service. I believe my prior experience in government and my more recent experience managing lawyers in a leading national law firm have prepared me well for the diverse challenges I would face if I am fortunate enough to be confirmed. I spent 17 years as a career federal prosecutor. In the course of that experience, I prosecuted everything from shoplifting cases to homicides, from narcotics conspiracies to sensitive public corruption cases. I also had an opportunity during my time at DOJ to work in the front office of the Criminal Division with then Assistant Attorney General

Michael Chertoff and others, and help oversee the Criminal Division's response to the attacks of 9/11.

With respect to the management of lawyers, my experience includes serving as Chief of the Criminal Division in the U.S. Attorney's Office in DC, which is the largest U.S. Attorney's Office in the country, and now, in private practice, managing the DC Office of a major law firm.

The General Counsel of DHS has a number of critical roles and challenging responsibilities. These include:

- providing legal advice to the Secretary and the senior leadership of the Department
- ensuring that the Department's policies and operations comply with Constitutional, statutory, and other legal and regulatory authorities, including laws that safeguard the fundamental rights and liberties of the American people
- leading and managing over 1800 lawyers, and doing so in a way that promotes morale, high performance, and efficiency.

If I'm confirmed, I would be honored to have an opportunity to work with, and in support of, the tens of thousands of dedicated men and women at DHS, who work day in and day out to carry out that vital mission.

One of the things I loved about being an Assistant U.S. Attorney was standing up in court and saying, "Steve Bunnell on behalf of the United States." I loved having the United States as my client. In fact, I loved it so much that after I left DOJ, when I first went to court as a defense

attorney, I stood up and introduced myself on the record as "Steve Bunnell on behalf of the United States." The judge was nice about it, but I was lucky that my client didn't fire me.

If I'm fortunate enough to be confirmed, one of the things that will mean a lot to me is once again being able to say -- accurately -- that I'm a lawyer for the United States. There is no better client a lawyer can have.

Mr. Chairman, thank you again for this opportunity to appear before you. I would be pleased to answer any questions that you may have.

REDACTED

HSGAC BIOGRAPHICAL QUESTIONS FOR EXECUTIVE NOMINEES

1. Basic Biographical Information

Please provide the following information.

Position to Which You Have Been Nominated

Name of Position	Date of Nomination
General Counsel, U.S. Department of Homeland Security	August 1, 2013

Current Legal Name

First Name	Middle Name	Last Name	Suffix
Stevan	Eaton	Bunnell	

Addresses

Residential Address (do not include street address)			Office Address (include street address)		
[redacted]			Street: O'Melveny & Meyers, 1625 Eye St. NW		
City: Washington	D.C.	Zip: 20015	City: Washington	D.C.	Zip: 20006

Other Names Used

First Name	Middle Name	Last Name	Suffix	Check if Maiden Name	Name Used From (Month Year) (Check box if estimate)	Name Used To (Month Year) (Check box if estimate)
					Est	Est

Birth Year and Place

Year of Birth (Do not include month and day.)	Place of Birth
1960	Ithaca, New York

Marital Status					
Check All That Describe Your Current Situation:					
Never Married	**Married**	**Separated**	**Annulled**	**Divorced**	**Widowed**
☐	X	☐	☐	☐	☐

Spouse's Name (current spouse only)			
Spouse's First Name	**Spouse's Middle Name**	**Spouse's Last Name**	**Spouse's Suffix**
Laura	Hume	Hills	

Spouse's Other Names Used (current spouse only)						
First Name	**Middle Name**	**Last Name**	**Suffix**	**Check if Maiden Name**	**Name Used From** (Month/Year) (Check box if estimate)	**Name Used To** (Month/Year) (Check box if estimate)
					Est ☐	Est ☐

Children's Names (if over 18)			
First Name	**Middle Name**	**Last Name**	**Suffix**
Philip	John	Hills-Bunnell	

2. Education

List all post-secondary schools attended.

Name of School	**Type of School** (vocational/technical/trade school, college/university/military college, correspondence/distance/extension/online school)	**Date Began School** (month/year) (check box if estimate)	**Date Ended School** (month/year) (check box if estimate) (check "present" box if still in school)	**Degree**	**Date Awarded**
Stanford Law School	University	Est ☐ 9/1983	Est ☐ Present ☐ 6/1986	JD	6/1986

Yale University	University	9/1978 Est.	5/1982 Est. Present	BA	5/1982

3. Employment

(A) List all of your employment activities, including unemployment and self-employment. If the employment activity was military duty, list separate employment activity periods to show each change of military duty station. Do not list employment before your 18th birthday unless to provide a minimum of two years of employment history.

Type of Employment (Active Military Duty Station, National Guard/Reserve, USPHS Commissioned Corps, Other Federal employment, State Government (Non-Federal Employment), Self-employment, Unemployment, Federal Contractor, Non-Government Employment (excluding self-employment), Other	Name of Your Employer/ Assigned Duty Station	Most Recent Position Title/Rank	Location (City and State only)	Date Employment Began (month/year) (check box if estimate)	Date Employment Ended (month/year) (check box if estimate) (check "present" box if still employed)
Non-government employment	O'Melveny &Meyers LLP	Managing Partner/Office Head (DC Office)	Washingt on, DC	3/2011	Present
Non-government employment	O'Melveny & Myers LLP	Partner	Washingt on, DC	9/2007	Present
Unemployment	Between jobs		Washingt on, DC	7/2007	9/2007
Other Federal employment	United States Attorney's Office, District of Columbia	Chief, Criminal Division	Washingt on, DC	7/2004	7/2007
Other Federal employment	United States Attorney's Office, District of Columbia	Chief, Fraud and Public Corruption Division	Washingt on, DC	4/2002	7/2004
Other Federal employment	Office of the Assistant Attorney General, Criminal Division, U.S. Department of Justice	Counsel to the Assistant Attorney General	Washingt on, DC	4/1999	4/2002
Other Federal employment	Public Integrity Section, U.S. Department of Justice	Trial Attorney	Washingt on, DC	4/1995	4/1999
Other Federal employment	United States Attorney's Office, District of Columbia	Assistant U.S. Attorney	Washingt on, DC	7/1990	4/1995
Non-government employment	Miller, Cassidy, Larocca & Lewin	Associate	Washingt on, DC	10/1987	7/1990
Unemployment	Between jobs		Washingt	7/1987	10/1987

			on, DC		
Other Federal employment	Judge Laurence H. Silberman, U.S. Court of Appeals, DC Circuit	Law Clerk	Washingt on, DC	7/1986	7/1987
Non-government employment	Yellow Taxi	Driver	New Haven, CT	12/1982	6/1983
Non-government employment	Yale University	Dishwasher/kitchen worker	New Haven, CT	9/1978 (during school year)	5/1982 (during school year)
Non-government employment	Town & Country Swimming Pools	Laborer	Poughkeepsie, NY	1979 (during summer)	1981 (during summer)

(B) List any advisory, consultative, honorary or other part-time service or positions with federal, state, or local governments, not listed elsewhere.

Name of Government Entity	Name of Position	Date Service Began (month/year) (check box if estimate)	Date Service Ended (month/year) (check box if estimate) (check "present" box if still serving)
United States Sentencing Commission	Practitioners Advisory Group, D.C. Circuit Representative	3/2011 Est ☒	Present Est
As a collateral duty while serving in the Office of the Assistant Attorney General, Criminal Division, U.S. Department of Justice	Adjunct Professor of Law at both Georgetown University Law Center & the George Washington University Law School	2000	2002

(C) Have you ever been fired from a job, quit a job after being told you would be fired, left a job by mutual agreement following charges or allegations of misconduct, left a job by mutual agreement following notice of unsatisfactory performance, or received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as violation of a security policy?

No.

4. Potential Conflict of Interest

(A) 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. I am not aware of any other potential conflicts of interest.

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

None.

5. Honors and Awards

List all scholarships, fellowships, honorary degrees, civilian service citations, military medals, academic or professional honors, honorary society memberships and any other special recognition for outstanding service or achievement.

In my current position, I have been named a leading lawyer in: *International Who's Who of Business Crime Lawyers* (2010-2011); a "Top Lawyer" by *Corporate Counsel* (2010-2011); named to *Expert Guides'* handbook of the "World's Leading White Collar Crime Lawyers" (2010); *Chambers USA* (2010-2013); and, listed in *Best Lawyers in America* (2009-2013).

At the U.S. Department of Justice, I received the Attorney General's Special Commendation Award in 1995. I also received numerous U.S. Department of Justice Special Achievement Awards, specifically: while serving as Counsel to the Assistant Attorney General I received this recognition in 2000 and 2001; while serving as a Trial Attorney, I received this recognition in 1996, 1997, 1998, & 1999; and, while serving as an Assistant United States Attorney I received this recognition in 1991 and 1993.

I graduated with distinction from Stanford Law School in 1986, where I served as the Senior Articles Editor of the Stanford Law Review, and was awarded the Hilmer Oehlmann Prize for outstanding legal writing. I graduated Magna Cum Laude from Yale University in 1982 and was selected for membership in the Phi Beta Kappa honorary society.

6. Memberships

List all memberships that you have held in professional, social, business, fraternal, scholarly, civic, or charitable organizations in the last 10 years.

Unless relevant to your nomination, you do NOT need to include memberships in charitable organizations available to the public as a result of a tax deductible donation of $1,000 or less, Parent-Teacher Associations or other organizations connected to schools

attended by your children, athletic clubs or teams, automobile support organizations (such as AAA), discounts clubs (such as Groupon or Sam's Club), or affinity memberships/consumer clubs (such as frequent flyer memberships).

Name of Organization	Dates of Your Membership (You may approximate.)	Position(s) Held
Metropolitan Club of Washington, DC	3/2011 to present	Member
Assistant United States Attorneys Association of Washington, DC	2002 to present	Member of Executive Committee/ Executive Counsel
Barristers	2004 to present	Member
Edward Bennett Williams Inn of Court	1989 to present	Treasurer (1999 to present); Barrister (1989 to present)
Just-Us Kids Childcare Center	1999 to 2007	Member, Board of Directors
Stanford Law School Board of Visitors	2008 to present	Member
American Bar Association	2007 to present	Member
Bar of the District of Columbia	1988 to present	Member

7. Political Activity

(A) Have you ever been a candidate for or been elected or appointed to a political office?

No.

Name of Office	Elected/Appointed/ Candidate Only	Year(s) Election Held or Appointment Made	Term of Service (if applicable)

(B) List any offices held in or services rendered to a political party or election committee during the last ten years that you have not listed elsewhere.

None.

Name of Party/Election Committee	Office/Services Rendered	Responsibilities	Dates of Service

(C) Itemize all individual political contributions of $200 or more that you have made in the past five years to any individual, campaign organization, political party, political action

committee, or similar entity. Please list each individual contribution and not the total amount contributed to the person or entity during the year.

Name of Recipient	Amount	Year of Contribution
Friends of Doug Gansler	$1000	2012
Friends of Doug Gansler	$1000	2011
Friends of Doug Gansler	$1000	2010
Glenn Ivey For Congress	$1000 ($578 of which was refunded in 2012)	2011
Friends of Glenn Ivey	$500	2008
Friends for Harry Reid	$1000	2010
Heidi for Senate	$1000	2012
Nebraskans for Kerry	$1000	2012
Bennet for Colorado	$1000	2010
Bennet for Colorado	$1000	2009
Klobuchar for Minnesota 2018	$1000	2011
O'Melveny & Myers PAC	$240	2012
O'Melveny & Myers PAC	$200	2011
Act Blue	$1000	2009
Obama Victory Fund 2012	$2500	2012

Obama Victory Fund 2012	$1000	2011
Obama for America	$1050	2008
Obama for America	$1000	2008
Obama for America	$1000	2008
Obama for America	$300	2008
Obama Victory Fund	$1000	2008
Obama Victory Fund	$250	2008
Udall for Colorado	$1000	2013

8. Publications and Speeches

(A) List the titles, publishers and dates of books, articles, reports or other published materials that you have written, including articles published on the Internet. Please provide the Committee with copies of all listed publications. In lieu of hard copies, electronic copies can be provided via e-mail or other digital format.

I have done my best to identify all titles, publishers and dates books, articles, reports or other published materials, including through a review of my personal files and searches of publicly available electronic databases. Despite my searches, there may be additional items that I have been unable to identify, find, or remember. I have located the following:

Title	Publisher	Date(s) of Publication
Negotiating Justice: Prosecutorial Perspectives on Federal Plea Bargaining in the District of Columbia	American Criminal Law Review	Summer 2006
In-House Counsel's Guide to Conducting Internal Investigations	O'Melveny & Myers Handbook	October 2010
New Incentives for Corporations to Maintain Effective Compliance and Ethics Programs	O'Melveny & Myers Client Alert	May 2010
Start Talking -- Or Else	Legal Times	August 2008
Internet Businesses Beware: Aggressive Enforcement of Money Laundering Laws Targets Online Payments Systems	O'Melveny & Myers Client Alert	July 2008

Stolt-Nielsen Finally Gets Amnesty	O'Melveny & Myers Client Alert	January 2008
Criminal Enforcement of Export Control/Sanctions Laws Announced as Top Priority of Justice Department and Partner Agencies Just as Higher Penalties Authorized	O'Melveny & Myers Client Alert	October 2007
The Use of Hypothetical Rates in Antitrust Damages Calculations: Reforming the Keogh Doctrine	Stanford Law Review	April 1986

(B) List any formal speeches you have delivered during the last five years and provide the Committee with copies of those speeches relevant to the position for which you have been nominated. Include any testimony to Congress or any other legislative or administrative body. These items can be provided electronically via e-mail or other digital format.

None.

Title/Topic	Place/Audience	Date(s) of Speech

(C) List all speeches and testimony you have delivered in the past ten years, except for those the text of which you are providing to the Committee.

I have been a frequent speaker at Bar conferences, Justice Department training courses, and given presentations to law school classes on issues relating to trial practice and federal prosecution. At these events I have spoken informally, and I have not given any formal speeches or provided any public testimony.

Title	Place/Audience	Date(s) of Speech
Corporate Plea Negotiations and Sentencing	National Federal Sentencing Guidelines Conference, Orlando, Florida	May 2011
Hot Topics in Corporate Internal Investigations	D.C. Bar CLE Presentation	October 2010
Corporate Plea Negotiations and Sentencing in a Post Thompson Memo World	National Federal Sentencing Guidelines Conference, St. Petersburg, FL	May 2010
Sentencing Practice and Procedure: Plea Negotiations, Charging Practices, Sentencing Tactics, and Victims' Rights	ABA Criminal Justice Section's Fall Program, Washington, DC	November 2009
Assessing and Managing the Risk of U.S. Law Enforcement Actions	O'Melveny/Deloitte Conference on the Re-Regulation of America "After the Financial Meltdown: The View of Washington, DC Insiders,"	October 2008

	Hong Kong	
Federal Plea Bargaining	Federal Bar Association and United States Sentencing Commission Annual Conference on the Federal Sentencing Guidelines, Orlando, FL	May 2008
Federal Law Enforcement Trends	Association of Corporate Counsel, Southern California Chapter, Los Angeles, CA	February 2008
Law Enforcement Issues in Export Control Investigations	TechNet Export Controls Conference, Santa Clara, CA	January 2008

9. Criminal History

Since (and including) your 18th birthday, has any of the following happened?

- Have you been issued a summons, citation, or ticket to appear in court in a criminal proceeding against you? (Exclude citations involving traffic infractions where the fine was less than $300 and did not include alcohol or drugs.)
    - o No
- Have you been arrested by any police officer, sheriff, marshal or any other type of law enforcement official?
    - o No
- Have you been charged, convicted, or sentenced of a crime in any court?
    - o No
- Have you been or are you currently on probation or parole?
    - o No
- Are you currently on trial or awaiting a trial on criminal charges?
    - o No
- To your knowledge, have you ever been the subject or target of a federal, state or local criminal investigation?
    - o No

If the answer to any of the questions above is yes, please answer the questions below for each criminal event (citation, arrest, investigation, etc.). If the event was an investigation, where the question below asks for information about the offense, please offer information about the offense under investigation (if known).

A) Date of offense:

a. Is this an estimate (Yes/No):

B) Description of the specific nature of the offense:

C) Did the offense involve any of the following?
   1) Domestic violence or a crime of violence (such as battery or assault) against your child, dependent, cohabitant, spouse, former spouse, or someone with whom you share a child in common: **Yes / No**
   2) Firearms or explosives: **Yes / No**
   3) Alcohol or drugs: **Yes / No**

D) Location where the offense occurred (city, county, state, zip code, country):

E) Were you arrested, summoned, cited or did you receive a ticket to appear as a result of this offense by any police officer, sheriff, marshal or any other type of law enforcement official: **Yes / No**

   1) Name of the law enforcement agency that arrested/cited/summoned you:

   2) Location of the law enforcement agency (city, county, state, zip code, country):

F) As a result of this offense were you charged, convicted, currently awaiting trial, and/or ordered to appear in court in a criminal proceeding against you: **Yes / No**

   1) If yes, provide the name of the court and the location of the court (city, county, state, zip code, country):

   2) If yes, provide all the charges brought against you for this offense, and the outcome of each charged offense (such as found guilty, found not-guilty, charge dropped or "nolle pros," etc). If you were found guilty of or pleaded guilty to a lesser offense, list separately both the original charge and the lesser offense:

   3) If no, provide explanation:

G) Were you sentenced as a result of this offense: **Yes / No**

H) Provide a description of the sentence:

I) Were you sentenced to imprisonment for a term exceeding one year: **Yes / No**

J) Were you incarcerated as a result of that sentence for not less than one year: **Yes / No**

K) If the conviction resulted in imprisonment, provide the dates that you actually were incarcerated:

L) If conviction resulted in probation or parole, provide the dates of probation or parole:

M) Are you currently on trial, awaiting a trial, or awaiting sentencing on criminal charges for this offense: **Yes / No**

N) Provide explanation:

10. Civil Litigation and Administrative or Legislative Proceedings

(A) Since (and including) your 18th birthday, have you been a party to any public record civil court action or administrative or legislative proceeding of any kind that resulted in (1) a finding of wrongdoing against you, or (2) a settlement agreement for you, or some other

person or entity, to make a payment to settle allegations against you, or for you to take, or refrain from taking, some action. Do NOT include small claims proceedings.

None.

Date Claim/Suit Was Filed or Legislative Proceedings Began	Court Name	Name(s) of Principal Parties Involved in Action/Proceeding	Nature of Action/Proceeding	Results of Action/Proceeding

(B) In addition to those listed above, have you or any business of which you were an officer, director or owner ever been involved as a party of interest in any administrative agency proceeding or civil litigation? 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.

None.

Date Claim/Suit Was Filed	Court Name	Name(s) of Principal Parties Involved in Action/Proceeding	Nature of Action/Proceeding	Results of Action/Proceeding

(C) For responses to the previous question, 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.

11. Breach of Professional Ethics

(A) Have you ever been disciplined or cited for a breach of ethics or unprofessional conduct by, or been the subject of a complaint to, any court, administrative agency, professional association, disciplinary committee, or other professional group? Exclude cases and proceedings already listed.

Name of Agency/Association/ Committee/Group	Date Citation/Disciplinary Action/Complaint	Describe Citation/Disciplinary Action/Complaint	Results of Disciplinary Action/Complaint

	Issued/Initiated		
Office of Professional Responsibility, U.S. Department of Justice	1996 (est.)	Acquitted criminal defendant alleged that she had been wrongly prosecuted, and I was part of the prosecution team.	Complaint found to be without merit.

(B) Have you ever been fired from a job, quit a job after being told you would be fired, left a job by mutual agreement following charges or allegations of misconduct, left a job by mutual agreement following notice of unsatisfactory performance, or received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as violation of a security policy?

No.

12. Tax Compliance

REDACTED

13. Lobbying

14

In the past ten years, have you registered as a lobbyist? If so, please indicate the state, federal, or local bodies with which you have registered (e.g., House, Senate, California Secretary of State).

No.

14. Outside Positions

☒ See OGE Form 278. (If, for your nomination, you have completed an OGE Form 278 Executive Branch Personnel Public Financial Disclosure Report, you may check the box here to complete this section and then proceed to the next section.)

For the preceding ten calendar years and the current calendar year, report any positions held, whether compensated or not. Positions include but are not limited to those of an officer, director, trustee, general partner, proprietor, representative, employee, or consultant of any corporation, firm, partnership, or other business enterprise or any non-profit organization or educational institution. Exclude positions with religious, social, fraternal, or political entities and those solely of an honorary nature.

Name of Organization	Address of Organization	Type of Organization (corporation, firm, partnership, other business enterprise, other non-profit organization, educational institution)	Position Held	Position Held From (month/year)	Position Held To (month/year)

15. Agreements or Arrangements

☒ See OGE Form 278. (If, for your nomination, you have completed an OGE Form 278 Executive Branch Personnel Public Financial Disclosure Report, you may check the box here to complete this section and then proceed to the next section.)

As of the date of filing your OGE Form 278, report your agreements or arrangements for: (1) continuing participation in an employee benefit plan (e.g. pension, 401k, deferred compensation); (2) continuation of payment by a former employer (including severance payments); (3) leaves of absence; and (4) future employment.

Provide information regarding any agreements or arrangements you have concerning (1) future employment; (2) a leave of absence during your period of Government service; (3)

continuation of payments by a former employer other than the United States Government; and (4) continuing participation in an employee welfare or benefit plan maintained by a former employer other than United States Government retirement benefits.

Status and Terms of Any Agreement or Arrangement	Parties	Date (month/year)

16. Additional Financial Data

REDACTED

SIGNATURE AND DATE

I hereby state that I have read the foregoing Statement on Biographical and Financial Information and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

This 27th **day of** August, **2013**

Subscribed and sworn to before me this 27th **day of** August **2013**

Signature of Notary Public

Notary Public, District of Columbia
My commission expires on June 14, 2014

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

SEP - 3 2013

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

In accordance with the Ethics in Government Act of 1978, I enclose a copy of the financial disclosure report filed by Stevan E. Bunnell, who has been nominated by President Obama for the position of General Counsel, Department of Homeland Security.

We have reviewed the report and have 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,

Don W. Fox
Principal Deputy Director

Enclosures **REDACTED**

August 23, 2013

Joseph Maher
Designated Agency Ethics Official
Department of Homeland Security
Washington, D.C. 20528-0485

Dear Mr. Maher,

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 General Counsel, 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.

Upon confirmation, I will withdraw from my position as a partner with the law firm of O'Melveny & Myers, LLP. For a period of one year after my withdrawal, I will not participate personally and substantially in any particular matter involving specific parties in which the firm is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d). I will not participate personally and substantially in any particular matter involving specific parties in which a former client of mine is a party or represents a party for a period of one year after I last provided service to that client, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d). Pursuant to a September 2007 O'Melveny & Myers, Limited Liability Partnership Agreement I will receive a lump sum partnership withdrawal payment, based on an objective formula, of the partnership income. In addition, I am a participant in the O'Melveny & Myers, LLP Defined Benefit plan. I am entitled to a cash refund from my contribution to the defined benefit plan which will be rolled into an individual retirement account. The amount of these payments will be fixed at the time of my withdrawal from the firm. Both of these payments will be made within 90 days of my confirmation. I will not participate personally and substantially in any particular matter that would have a direct and predictable affect on the ability or willingness of O'Melveny & Myers, LLP to make these payments to me, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1). I am also a participant in the O'Melveny & Myers, LLP Defined Contribution Keogh Plan. The assets in this plan will be rolled into an individual retirement plan.

I currently have a capital account with O'Melveny & Myers, LLP and I will receive a refund of the account after my withdrawal. Until I have received this refund, I will not participate personally or substantially in any particular matter that will have a direct and predictable effect on the ability and willingness of the firm to pay this refund, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b) (1).

My spouse and I will divest our interests in our Capital One managed account within 90 days of my confirmation (see attached list). With regard to each of these entities, I will not participate personally and substantially in any particular matter that has a direct and predictable effect on the financial interests of the entity until I have divested it, 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).

Upon confirmation, I will resign my position of Treasurer, Edward Bennett Williams Inn of Court and Executive Committee member position with the Assistant United States Attorney Association. For a period of one year after my date of resignation, I will not participate personally and substantially in any particular matter involving specific parties in which the Edward Bennett Williams Inn of Court or Assistant United States Attorney Association is a party or represents a party, unless I am first authorized to participate pursuant to 5 C.F.R. § 2635.502(d).

My spouse is currently a partner with the law firm of Hills & Morley, LLP. I will not participate personally and substantially in any particular matter that has a direct and predictable effect on the financial interest of the firm, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b) (1). I also will not participate personally and substantially in any particular matter involving specific parties in which the firm or any client of my spouse is a party or represents a party, unless I am first authorized to participate, pursuant to 5 C.F.R. § 2635.502(d). In addition, for the duration of my appointment to the position of General Counsel, my spouse has agreed not to communicate with the Department of Homeland Security on behalf of the firm or any client.

I have been advised that this ethics agreement will be posted publicly, consistent with 5 U.S.C. §552, on the website of the U.S. Office of Government Ethics with other ethics agreements of Presidential nominees who file public financial disclosure reports.

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 and any other ethics agreement.

Sincerely,

Stevan E. Bunnell

U.S. Senate Committee on Homeland Security and Governmental Affairs
Pre-hearing questionnaire for the nomination of
Stevan E. Bunnell to be
General Counsel, Department of Homeland Security

I. Nomination Process and Conflicts of Interest

1. Why do you believe the President nominated you to serve as General Counsel at the Department of Homeland Security (DHS)?

I believe I was nominated for the position of General Counsel for the Department of Homeland Security (DHS) because of my qualifications, which include over 25 years of experience practicing law and managing lawyers in the public and private sectors, 17 years of experience as a career federal prosecutor in the U.S. Attorney's Office for the District of Columbia and the Criminal Division of the Department of Justice, and my strong legal ability, leadership, and other personal qualities.

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

No.

3. Have you made any commitments with respect to the policies and principles you will attempt to implement as General Counsel? If so, what are they and to whom have the commitments been made?

No, other than an implicit commitment to support and defend the Constitution and to take care the laws of the United States are faithfully executed, to the best of my ability.

4. 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 you will use to carry out such a recusal or disqualification.

In connection with the nomination process, I have consulted with the Office of Government Ethics and DHS'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.

II. Background of the Nominee

5. What specific background and experience affirmatively qualifies you to be General Counsel?

Specific background and experiences relevant to my qualifications to be the General Counsel of DHS include:

- *Over 17 years of experience as a career federal prosecutor, including experience as a line prosecutor in the U.S. Attorney's Office for the District of Columbia, where I prosecuted both federal and local criminal cases, and experience as a Trial Attorney in the Public Integrity Section of the Department of Justice, where I investigated and prosecuted numerous sensitive public corruption cases in federal jurisdictions around the country.*

- *Over eight years of private practice experience, handling criminal and civil litigation, as well as corporate internal investigations and compliance issues. My private practice experience has included sensitive and challenging work for some of the nation's leading public and private companies, and has included regulatory, enforcement, and data privacy issues.*

- *A record of successfully managing large groups of lawyers in both the public and private sectors, including management experience in the public sector as Chief of the Criminal Division of the DC U.S. Attorney's Office, where I oversaw a staff of 130, including 85 AUSAs, Chief of the Fraud and Public Corruption Section of the DC U.S. Attorney's Office where I supervised approximately 25 AUSAs, and Counsel to the Assistant Attorney General for the Criminal Division at DOJ, where I advised on management decisions, executed strategic plans, and routinely lead inter-agency working groups; and management experience in the private sector, where I currently manage the Washington, DC office of O'Melveny & Myers LLP, which is an office with a staff of approximately 180, including more than 110 attorneys.*

- *Extensive experience with national homeland security issues, including during my tenure as Counsel to the Assistant Attorney General of the Criminal Division at DOJ, working closely with then Assistant Attorney General Michael Chertoff and others to shape the Criminal Division's response to the attacks of September 11, 2001; helping to draft DOJ's initial guidance to implement information sharing provisions of the USA PATRIOT Act; serving as the lead Criminal Division staff representative on the Interagency Commission of Crime and Security in U.S. Seaports; organizing a training conference for federal law enforcement agents and prosecutors on combating corruption along the Southwest Border; and representing the Criminal Division on an inter-agency working group to combat leaks of classified information.*

- *Strong legal acumen and practical judgment necessary to perform with distinction at the highest levels of government, as demonstrated by my success as a partner in a major national law firm, my senior leadership roles as a career federal prosecutor, my experiences as a law clerk for the U.S. Court of Appeals for the District of Columbia Circuit, and my academic record.*

6. How would you describe your leadership and management style?

My leadership and management style is both strategic and people-focused. In my leadership roles, I have focused first on setting a personal example of integrity, excellence, and dedication to the mission of the organization. For example, as Chief of the Criminal Division in the U.S.

Attorney's Office, I routinely stepped back from the details of a particular decision to consider, and to ask those working with me to consider, whether a particular course of action was consistent with the obligations of a federal prosecutor to seek justice and do so in a just way. As an office leader in a national law firm with a 127-year history, I seek to be a steward of the firm's best traditions and try to pass on the firm's values of excellence, citizenship, and leadership to the next generation of firm lawyers. I regularly articulate to my firm colleagues how seemingly routine work can ultimately contribute to those values and traditions.

My experience leading and managing lawyers has taught me the critical importance of establishing and prioritizing personal connections with the people I lead. I attempt to do this in part through the accumulation of numerous small personal actions and gestures. For example, I am a firm believer in the value of management by walking around, and I do it frequently -- stopping by people's offices, asking them what they are working on, thanking them for their efforts, listening to what they find rewarding and what they find frustrating about their work, and asking how I can help them be more successful and develop professionally. I look for opportunities to praise and thank, to offer support and reassure when needed, to coach, and to reward high performance with greater professional opportunities and responsibilities. I believe that lawyers in both the public and private sectors are motivated less by financial reward than by a sense that their work is significant and respected, that they have a degree of autonomy, and that they are appreciated.

My approach to leadership/management also emphasizes transparency and communication. Open and straightforward communication from leaders not only breeds trust and engagement, it also leads to a more robust exchange of viewpoints, which ultimately leads to better decisions, higher morale, and greater productivity.

7. In what ways, if any, do you believe the role, responsibilities and obligations of a government lawyer are different from those of a private-sector lawyer? How do you see your role of General Counsel at DHS, if you are confirmed, as different from that of your past roles at the U.S. Attorney's Office for the District of Columbia and as a partner at a law firm?

A government lawyer must typically represent a broader set of interests than a private-sector lawyer whose client is an individual or a corporate entity. A lawyer in the federal government has a responsibility to represent not only the immediate interests of the agency that he or she is working for, but also the larger interests of the United States, which are grounded in the Constitution, the institutions of government, and the wider public interest. In my past role as a federal prosecutor, my obligation was not merely to win cases it was to make decisions based on the facts, the law, and DOJ policy, and ultimately to see that justice was done in a way that respected the rights of all concerned. It was to those obligations that I was ultimately held accountable. In private practice, my role has frequently been to be an advocate for the best interests of a private party, which can sometimes be challenging and complex to determine (especially in the context of corporate representations), but which ultimately is a narrower and more limited role than that of a government lawyer.

8. Please describe any of your previous work on privacy or civil liberties issues and highlight experience that you think will be particularly relevant to privacy concerns you would face as DHS General Counsel.

As a federal prosecutor, I had an obligation to ensure that the investigations and prosecutions I handled or supervised were conducted in a manner that did not unlawfully or otherwise unduly infringe on the privacy or other rights of victims, witnesses, and defendants. For example, in the course of conducting federal grand jury investigations, I regularly collected and had access to sensitive or highly personal information, including information obtained through electronic surveillance and other covert investigative methods. I took very seriously my obligations to maintain the secrecy of such information and to use it only for the limited purposes for which it was authorized. In addition, as a federal prosecutor in the Public Integrity Section, I developed an expertise in public corruption cases, including cases in which law enforcement officials violated their duties to the people they had sworn to serve. In private practice, I have represented individuals who have felt the intrusive force of an intensive federal criminal investigation, and I have represented companies that have experienced a breach of personally identifiable information, and have counseled those clients on enhancements to their internal systems for the management of such information. I believe these diverse experiences have sensitized me to the importance and the challenge of balancing operational effectiveness with the imperative of protecting the privacy interests and civil liberties of citizens who may be affected by DHS's work.

III. Role of the General Counsel at the Department of Homeland Security

9. How do you view the role of General Counsel at DHS?

The General Counsel has many roles. As the chief legal officer of the Department, the General Counsel is responsible for providing legal advice and services to the Secretary and the leadership team of the Department and its component agencies. The General Counsel is also responsible for leading and managing the operations of the Legal Department, and ensuring that the legal advice and services provided are of high quality, responsive, practical, and timely in a way that advances DHS's overall missions. The General Counsel is also responsible for ensuring that the Department complies with applicable laws, regulations, and other legal authorities, including, but not limited to compliance with laws protecting civil liberties and privacy, congressional oversight requirements, and requests from the Government Accountability Office (GAO) and the Department's Inspector General. In addition, I believe that the General Counsel can and should play a broader role in helping to promote and institutionalize a culture of collaboration and coordination both within DHS's components and in relationships with other departments and agencies of the Executive Branch.

10. If confirmed, what will be the immediate highest priority legal issues that you expect to address? What longer-term goals would you like to achieve in your tenure as General Counsel?

If I am confirmed, the highest priority legal issues will flow from the Secretary's priorities for the Department and will depend upon the circumstances and challenges presented to the Department. These issues will undoubtedly involve the specific missions of the Department as set out in the Homeland Security Act, including advising on legal issues associated with efforts to prevent terrorist attacks and securing the Nation's borders and critical infrastructure. I am aware that the Administration continues to work with Congress on legislation involving the important areas of cybersecurity and immigration reform. Progress in those areas, and implementation of the President's recent Executive Order related to cybersecurity, will present many legal issues. In addition, the development of new technologies that aid the homeland security mission—in air transportation screening, border surveillance, cybersecurity, and information sharing, to name just a few—will continue to present legal issues during program development. Ensuring adherence to Constitutional and statutory requirements, while enhancing the mission capabilities of the Department, will require careful legal analysis and advice.

In the longer term, if confirmed, I would want to ensure that the Office of the General Counsel has a strong foundation to provide high quality and timely legal advice throughout the organization. This will require strong coordination throughout that office and the Department, the ability to recruit and retain excellent lawyers, and a shared commitment to the rule of law and the missions of the Department.

11. What do you believe is the appropriate relationship between the DHS Office of General Counsel and component legal departments?

As I understand the structure of the legal offices within DHS, as set out by Secretarial delegations and directives, the Office of the General Counsel includes both a headquarters element and the offices that reside in the components. The Department's directives require these offices to report to the General Counsel, except where otherwise provided in statute (such as with the attorneys providing legal counsel for the Inspector General). I believe that this type of organizational structure promotes functional accountability and enhances consistency of legal interpretations throughout a large organization like DHS. Strong coordination and frequent communication among the various offices within the Office of the General Counsel will be essential to promoting that consistency while serving the legal needs of the various officials throughout a large department.

12. What steps will you take to ensure consistency of legal positions across the Department, including in its components?

The General Counsel is the chief legal officer of the Department, and ultimately has final authority and responsibility for legal policy determinations within the Department and its components. The Office of the General Counsel represents the Department in many different legal forums, so it is imperative that legal interpretations are applied consistently and

communicated across the Department. If confirmed, I would like to review the processes that the Office of the General Counsel uses to develop and communicate legal positions, especially in areas that are cross-cutting, including positions in litigation or on proposed legislation, the development of regulations, and the interpretation of existing laws.

IV. Policy Questions

General Legal Issues, Management, and Mission Support

DHS Authorities

13. In many areas, the responsibilities of DHS intersect, and at times overlap, with those of other cabinet departments. In addition, in a number of areas, such as disaster planning and response, DHS has been given the responsibility to coordinate federal efforts across agencies. Do you believe that DHS has sufficient, and sufficiently clear, legal authorities for the Department to act effectively in the interagency context?

The Homeland Security Act, as amended, and other authorities such as Homeland Security Presidential Directives, Presidential Policy Directives, and Executive Orders provide DHS with many specific responsibilities with regard to protecting the homeland. Because many of the Department's activities intersect with the missions of other departments and agencies, I believe that the Department must cooperate and coordinate with other departments and agencies to ensure that the Department is successful in fulfilling its many responsibilities. From my preliminary review of the Department's authorities, I believe the Department's legal authorities are sufficient, and sufficiently clear, to allow effective and productive action in the interagency context. If confirmed, I will be able to better discern how those legal authorities are construed and employed in the interagency on a day-to-day basis.

Congressional Oversight

14. Other than a valid claim of executive privilege, on what bases, if any, do you believe the Department may be entitled to withhold information or documents from Congress? Please explain the legal authority for your view.

I believe that oversight is not only an important authority necessary for Congress to fulfill its Constitutional duties, but vital to the proper functioning of the Executive Branch.

If confirmed, I intend to strive to make sure that the Department is responsive to valid Congressional requests for information including appropriate access to the information it seeks as part of its oversight of the Department.

15. Under what circumstances, if any, do you believe an official or employee of the Department may decline to testify before a Congressional Committee? Please explain the legal basis for your conclusion.

In my view, appearing before Congress when invited is one of the duties of an Executive Branch official. Given the importance of Congress's legislative and oversight responsibilities, I believe it would be very rare for the Department to decline to make an official or employee of the Department available to testify before a Congressional Committee. Even in exceptional situations where, hypothetically, the Department believed that the mere appearance of a particular employee witness would impair a vital Departmental interest (e.g., a sensitive pending law enforcement investigation or a critical national security interest), I would expect that through consultation an accommodation could be reached that would satisfy the Committee's interests. Of course all congressional witnesses, including government employees, have a personal right under the Fifth Amendment of the Constitution to decline to testify to avoid self-incrimination, but that is a personal right that could not be asserted by the Department. It would have to be asserted personally by the individual witness, typically on the advice of personal counsel.

16. What criteria should the Office of General Counsel use to decide whether and how to respond to requests from Congress for documents, information, or testimony?

As a general matter, the Office of the General Counsel should operate under the presumption that it should cooperate with Congressional oversight and be responsive to appropriate requests from Congress for documents, information, or testimony. If confirmed, I intend to operate under this principle. Of course, the Office's ability to be responsive will also depend upon such factors as the breadth and specificity of the requests at issue; the degree to which responsive information exists and is accessible in a responsive format within a reasonable timeframe; the ability of requesters to prioritize what may be multiple competing requests; the need to accommodate circumstances involving classified information or truly privileged communications; and the capacity of the Office to respond to all requests in a prompt and coordinated manner. I believe that open communication with Congress is vital, and if I am confirmed I intend to ensure that any such issues are discussed and shared with Congress in an effort toward finding ways for Congress to satisfy its oversight responsibilities.

Whistleblowers

17. Whistleblowers continue to be an important way Congress, agencies and Inspectors General receive complaints regarding waste, fraud and abuse.

    a. How would you define a whistleblower?

Under federal law, a whistleblower may be a current or former federal employee, or an applicant for federal employment who discloses information to Congress, the Office of Special Counsel, the Office of the Inspector General, or another employee designated by the head of the agency to receive such disclosures that the whistleblower reasonably believes evidences

violations of a law, rule or regulation, gross mismanagement; a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

b. During your career have you dealt with whistleblowers? If so, provide some examples.

As a federal prosecutor, I regularly handled or supervised investigations and prosecutions of fraud and public corruption cases that originated from a whistleblower complaint. I know from personal experience how important whistleblowers are to investigators and prosecutors as inside sources of government fraud and other abuses within federal agencies, and how important it is to provide a process that encourages and protects whistleblowers who come forward with such information. When I was Chief of the Fraud and Public Corruption Section in the DC U.S. Attorney's Office, I met regularly with the head of the Office's Affirmative Civil Enforcement program (ACE) to coordinate the government's civil and criminal interests in False Claims Act allegations made by whistleblowers. I also have had extensive experience in private practice with whistleblowers and potential whistleblowers in the corporate context. Many of the internal investigations that I have conducted for corporate clients originated from calls to internal ethics hotlines or reports by current or former employees to a government regulatory or investigative agency. My experience in the private sector has primarily involved whistleblower issues in the areas of healthcare and government contracting fraud.

c. What do you believe is the proper way the DHS Office of General Counsel should handle whistleblowers?

The Office of the General Counsel should refer whistleblower complaints it receives to the appropriate officials, such as the Office of the Inspector General or the Office of Special Counsel, pursuant to applicable statutory and departmental directives. The Office of the General Counsel should further advise DHS officials to observe all legal prohibitions against retaliation related to whistleblowers. Also, the Office of the General Counsel should advise any individual claiming to have been retaliated against because of a protected disclosure of the individual's right to file a complaint with the Office of Special Counsel.

d. If confirmed, how would you mitigate any potential retaliation against a whistleblower?

Federal law sets out strong protections for employees who bring to light fraud, waste, and abuse in the government. If confirmed, I would reinforce to supervisors and leadership that they may not retaliate against whistleblowers under applicable law.

Government Accountability Office

18. What do you see as the Department's responsibilities to accommodate the Government Accountability Office (GAO) in carrying out its audits and investigations? Do you believe there are legitimate reasons to withhold documents from GAO? If so, what are those reasons?

I believe DHS should be fully committed to cooperating with GAO in its reviews. GAO performs an important role in our constitutional system of government, which I know the Department recognizes and supports, as do I.

I understand that former DHS General Counsel Ivan Fong devoted considerable time and energy during his tenure, working closely with others, both inside and outside the Department, to help build and strengthen the Department's relationship with GAO in a mutually beneficial and productive manner. This included the leadership of the Management Directorate, to whom the Secretary of Homeland Security has delegated overall responsibility for DHS relations with GAO, and under whose supervision and oversight the Departmental GAO-OIG Liaison Office functions. If confirmed, I intend to continue and build on my predecessor's success in this area by continuing to focus on engagement, responsiveness, and mutual respect between the Department and GAO.

It is important for the Department to be responsive to GAO requests, and if confirmed, I would work to facilitate the timely production of responsive information to GAO. Congress has given GAO broad statutory rights of access to a wide range of department and agency documents. It is my understanding that this access is nonetheless subject to a few narrow statutory exceptions, such as if: 1) the document relates to activities the President designates as foreign intelligence or counterintelligence activities; 2) the document is specifically exempted from disclosure to the Comptroller General by statute; or 3) the President or the Director of the Office of Management and Budget certifies that disclosure of the document "reasonably could be expected to impair substantially the operations of the Government" and that the document could be withheld under either 5 U.S.C. § 552(b)(5) (certain deliberative process documents) or (b)(7)(certain law enforcement documents). In general, however, I believe that in the vast majority of cases, the Department and GAO can reach an accommodation to provide GAO with the information that it seeks.

DHS Inspector General

19. What do you see as the Department's responsibilities to accommodate the Inspector General in carrying out audits and investigations? What do you see specifically as the General Counsel's role in this regard?

During my tenure as a federal prosecutor in the Public Integrity Section at DOJ and as Chief of the Fraud and Public Corruption Section of the DC U.S. Attorney's Office, I worked extensively with multiple federal inspector general offices. I understand and respect the important and independent role the Inspector General has within the Department and would make every effort to ensure DHS personnel cooperate with Office of Inspector General staff to further promote efficiency and effectiveness in DHS programs and operations.

More specifically, my view on this issue comports with long standing Department guidance issued by former Secretary of Homeland Security Michael Chertoff. This guidance emphasizes the expectation that all DHS employees will cooperate fully with the Office of the Inspector General regarding audits and investigations and shall provide prompt access to requested materials and information.

If confirmed, I see the Office of the General Counsel's role in these interactions as: 1) helping ensure that DHS employees cooperate fully with the inspector general inquiries and investigations; and 2) advising on laws and directives related to interactions with the Office of the Inspector General.

Ethics

20. The Office of the General Counsel has responsibility for helping to ensure DHS employees avoid conflicts of interest. What measures will you put in place to help identify and prevent potential conflicts of interest, or the appearance of such conflicts, among DHS employees?

As with all Executive branch agencies, DHS has appointed a Designated Agency Ethics Official (DAEO) to coordinate and manage the Department's Ethics Program as required by U.S. Office of Government Ethics regulations. Under the guidance of the DAEO, the Ethics Program provides advice, counseling, and training to DHS employees relating to an employee's obligation to comply with the Standards of Ethical Conduct for Employees of the Executive Branch, and related regulations and criminal statutes. The Ethics Program also sustains a financial disclosure reporting program for employees in compliance with regulations and DHS policy in order to avoid an actual conflict of interest or an appearance of the same. It is my understanding that the DAEO is currently housed organizationally in the Office of the General Counsel. If confirmed, I intend to work in close coordination with the DAEO to help identify and prevent potential conflicts of interest, or the appearance of such conflicts, among DHS employees.

Workforce

21. One of the principal challenges facing the Department is personnel management. As a relatively new agency, the Department must continue to enhance the integration of the various components into a cohesive department. What do you believe should be the role of the General Counsel in addressing these challenges, and what specifically do you intend to do in this area if confirmed?

If confirmed, I intend to fully support and provide legal advice to the Secretary and Under Secretary for Management on personnel management issues. By providing accurate and timely legal advice regarding labor and employment matters, I would support efforts by the Department's senior leaders and human capital staff to improve strategic human capital initiatives, protect the rights and liberties of employees within the Department, and uphold ethical standards during the execution of human capital activities across the Department.

Freedom of Information Act

22. The Freedom of Information Act (FOIA) plays a critical role in ensuring the integrity of our government and the vitality of our democracy. If confirmed, what will you do to ensure that the Department and all of its component agencies properly and efficiently comply with FOIA?

I am committed to the spirit and letter of federal disclosure laws including the Freedom of Information Act (FOIA). If confirmed, I will work closely with the Chief Privacy Officer, who also serves as the Chief FOIA Officer and is responsible for the Department's compliance with FOIA and its deadlines, to ensure that Department lawyers are working with the Chief Privacy Officer and his or her staff to help the Department fully comply with statutory disclosure obligations. The Department should strive to make appropriate information available to the public, and I will promote transparency in carrying out the mission of the Department.

I have been told that the ongoing collaboration between the Office of General Counsel, Chief FOIA Officer, and Component FOIA offices has led to a decrease in the Department's FOIA backlog. If I am confirmed I will work closely with the Department's Chief FOIA Officer to maintain that commitment.

Privacy and Civil Liberties

23. The creation of the Department raised many concerns over how the privacy and civil liberties of Americans would be affected by new initiatives to prevent terrorism. To address these concerns, the Homeland Security Act established a Privacy Office and the Office of Civil Rights and Civil Liberties at DHS.

    a. How should the Office of General Counsel work with and support the missions of these two offices?

The Office of the General Counsel has, to my understanding, provided legal support to both the Office for Civil Rights and Civil Liberties (CRCL) and the Privacy Office since their creation. I further understand that senior officials from the Office of the General Counsel, the Privacy Office, and CRCL meet on a regular basis to discuss ongoing projects with each office, and specific issues that can further the missions of all three offices. It is important that the Department's lawyers work closely with CRCL and Privacy staff to ensure that the Department complies with applicable laws and regulations, including laws protecting civil rights, civil liberties, and privacy. It is my belief that protection of civil rights, civil liberties, and privacy rights is wholly compatible with the Department's mission to secure the homeland.

    b. What role do you envision for yourself, as General Counsel, in overseeing compliance with privacy laws?

As with all the other laws with which the Department must comply, I see the Office of the General Counsel working with operational components and the Chief Privacy Officer to regularly review Department policies and operations and to provide legal advice and guidance on issues facing the Department that affect the privacy of individuals. Likewise, I will work to ensure that Department operations are respectful of individual privacy rights and interests and that the Department acts responsibly and is accountable for the appropriate collection and use of personal information.

    c. Can you identify areas where you believe DHS needs to take additional steps in order to ensure the protection of privacy and fundamental liberties?

I am not privy to all the details regarding the Department efforts to protect privacy and fundamental liberties. If confirmed, I will work closely with the Chief Privacy Officer, the Officer for Civil Rights and Civil Liberties, and the Department components to provide advice on carrying out their respective missions in a way that is respectful of privacy and civil liberties. Although I am not yet aware of all of the Department's operations, I note that the continual development of new technologies and capabilities creates both an opportunity and a challenge. New technologies provide the Department with unprecedented capacity to accomplish its mission, but also present new challenges with respect to the protection of privacy and fundamental liberties. I am confident that should I be confirmed, I will be able to work with the Chief Privacy Officer to address these challenges as they arise.

Acquisitions

24. What role do you believe the Office of the General Counsel should play in ensuring that the Department's acquisitions comply with the Federal Acquisition Regulation and Departmental rules and policies governing acquisitions?

The Office of the General Counsel plays a critical role in ensuring that the Department's acquisitions comply with applicable federal laws and regulations. I believe that it is vital that the Department's attorneys not merely advise acquisitions passively, but be an active part of the team that is responsible for making acquisition decisions, providing legal advice to program officials, budget personnel, and procurement officials, and helping them to develop an acquisition strategy, assist in the development of the contracting documentation, such as the solicitation and the award documents, and review the documentation to ensure legal compliance.

25. The Department has made steady progress in increasing the rate of competition in its spending on contracts. What steps do you believe could be taken within the Department to continue this progress and strengthen the use of competition when procuring goods and services?

I understand that the Department has made great progress in increasing its competitively-awarded contracts. As the Department continues these efforts and works to expand initiatives to maximize competition, if confirmed as General Counsel, I will ensure that the Office of the General Counsel maintains its involvement as an integral part of DHS's contracts and procurement framework. I would aim to provide the best guidance to ensure that DHS's contracts and procurement practices comply with federal laws and regulations, while promoting transparency and delivering the best value product or service to the customer within the Department's financial and legal constraints.

Rulemaking

26. The Office of General Counsel plays a large role with respect to rulemaking. It leads the Department's rulemaking activities, coordinates review of proposed regulations, and ensures that all regulatory actions presented to the Secretary comply with constitutional and statutory restrictions and mandates.

a. Please discuss your experience to date with the federal regulatory process.

In private practice, I have handled many matters that included regulatory compliance or enforcement issues. As part of my work on those matters, I have had to interpret federal regulations and analyze the rulemaking process from which they emerged. I also was a law clerk for a Judge on the U.S. Court of Appeals for the D.C. Circuit, and in that role worked on numerous appeals of administrative rulemakings. I am confident that if confirmed I could effectively lead the Department's rulemaking activities by leveraging the rulemaking expertise that presently exists within OGC, supplementing that expertise with additional resources if necessary, and by deepening my personal knowledge of the key legal and management issues associated with the rulemaking process.

b. If the Senate-passed comprehensive immigration reform legislation becomes law, the Department will face daunting implementation challenges. How would you approach the challenge of conducting multiple, significant rulemakings in a short timeframe?

If the Senate-passed comprehensive immigration reform were to become law, it would result in the need for numerous rulemakings, including many that would be considered significant under Executive Order 12866, "Regulatory Planning and Review." It is likely that these rulemakings would be complex, technical, and required on short timeframes. As with all regulatory actions, these would require a careful and deliberate consideration of the policy and operational implications, and an analysis of the costs and benefits. DHS has a robust regulatory program that would be leveraged to respond to the challenges posed by the need to issue numerous, complex regulations in a short timeframe. DHS would take those steps necessary to resource the development of these important, new immigration regulations.

Prevent Terrorism and Enhancing Security

Information Sharing

27. The Department faces a constant challenge in balancing the need to protect valuable intelligence sources and methods with the need to produce useful intelligence products at the lowest possible classification so that they can be disseminated as necessary. Although the Intelligence Community continues to undergo a cultural transformation toward a "need to share" principle, there remains a concern that some valuable information is "over-classified." If confirmed, how will you work with the Office of Intelligence and Analysis to develop policies and procedures that encourage the appropriate classification of Department intelligence products?

I am not privy to all the details regarding the Department's Intelligence Community activities; however, I understand that efforts for sharing intelligence and analysis at the lowest possible classification level with state, local, territorial, and tribal law enforcement as well as the private sector is one of the most critical efforts of DHS. This is an effort not without challenges, since protecting sources and methods is critical to Intelligence Community agencies' ability to collect

information, and also because DHS's domestic role means that it must work diligently to ensure that the civil rights, civil liberties, and privacy of U.S. Persons are protected.

If confirmed, I will work with the Office of Intelligence and Analysis and across the Department to build upon current efforts to ensure appropriate classification of intelligence information and analytic products.

28. Fusion centers bring together federal, state, and local agencies and regularly handle both law enforcement information and national intelligence. However, this co-location and integration also creates potential new legal issues and concerns.

    a. Do you believe that there is sufficient legal and policy guidance for state and local fusion centers today? If not, what additional guidance is needed?

I understand that the federal government recognizes that fusion centers are owned and operated by state and local agencies. However, I have been informed that the federal government supports fusion centers in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding. Although I am not aware of all of the Department's activities in this area, I believe existing law provides DHS with an adequate framework for the Department's engagement with fusion centers. Furthermore, the National Strategy for Information Sharing (2007) and the National Strategy for Information Sharing and Safeguarding (2012) both provide detailed policy guidance for the federal government's support for and engagement with fusion centers.

    b. If confirmed, what role do you expect the Office of General Counsel to play in assessing and addressing potential privacy and civil liberties impacts, as well as other legal issues, associated with fusion centers?

The Office of the General Counsel will continue to work with all appropriate partners in providing guidance for DHS's engagement with the National Network of Fusion Centers. This includes working with the Office of Intelligence and Analysis, which is responsible for coordinating federal efforts to engage with fusion centers, as well as the Privacy Office and the Office for Civil Rights and Civil Liberties. This engagement also extends into the provision of training (including privacy, civil rights, and civil liberties training) to federal, state, and local partners involved in fusion centers, as well as the review of products jointly produced by DHS and fusion centers.

It is my understanding that the Office of the General Counsel is a sitting member of the DHS Information Sharing and Safeguarding Governance Board's Fusion Center Executive Steering Committee (ESC). This Steering Committee provides a formalized governance process for Departmental engagement with and support for fusion centers.

    c. On March 13, 2013 the Government Accountability Office released a report (GAO-13-233) assessing the Nationwide Suspicious Activity Reports (SAR) Initiative. This audit revealed that three fusion centers were only using Shared Spaces system to log their SARs while twenty fusion centers only use the unclassified version of the

FBI's Guardian system (eGuardian) for logging SARs. The rest of the fusion centers were using some combination of Shared Spaces and eGuardian to report their SARs. One of the reasons cited for this split between the two systems was that Shared Spaces allowed for greater compliance with local and state privacy laws. This existence of separate reporting tracks could impede the ability of fusion centers to effectively share terrorism related suspicious activity reports with the federal government. What steps can the Office of General Counsel take to help ensure that privacy challenges that fusion centers face are minimized so that terrorism related information can be shared in a timely manner?

I understand that the federal government recognizes that fusion centers are owned and operated by state and local agencies, and therefore must comply with their own local laws. In order to ensure that fusion centers are able to report suspicious activities to the federal government in a manner that is consistent with their laws, the federal government supports their use of whichever of the two systems allows compliance with these local laws. If confirmed, I will work with interagency partners to continue to evaluate these systems and associated processes to ensure this information is shared in the most effective and efficient manner, while protecting privacy, civil rights, and civil liberties, and supporting state compliance with all of their own local laws.

29. The Office of Civil Rights and Civil Liberties (CRCL) conducts community engagements as part of their countering violent extremism mission. What role does the Office of General Counsel play in reviewing this office's activity to ensure that CRCL's engagements are both effective and adhering to the law and DHS privacy standards?

Community engagement is a core function of the Office for Civil Rights and Civil Liberties (CRCL). I generally understand that community engagement is a tool used by CRCL to communicate information to the public about federal programs and policies. I also understand that CRCL uses community engagement to obtain information from the public that CRCL then incorporates into the policymaking process as it relates to civil rights and civil liberties, and to deepen channels of communication between communities and federal officials in order to facilitate solution of problems. Indeed, keeping the public informed as to the activities of the Officer is one of CRCL's statutory responsibilities. I have been informed that there are attorneys dedicated to providing legal support to CRCL, and if confirmed I look forward to learning more about how CRCL uses community engagement as part of the Department's activities in countering violent extremism. If confirmed, I commit to ensuring that CRCL's activities are carried out in a legal manner.

SAFETY Act

30. Under the "Support Anti-Terrorism by Fostering Effective Technologies Act," or SAFETY Act (P.L. 107-296 Subtitle G), the Secretary may designate "qualified anti-terrorism technologies" to qualify for legal liability protections. The Act is administered by DHS's Science and Technology Directorate. What role do you think the Office of the General Counsel should play in the SAFETY Act application process?

The Office of General Counsel should play an active part in the SAFETY Act process. The SAFETY Act is unusual in that it empowers the Department to confer legal benefits on companies and products. For that reason alone, it is vital that OGC be involved at every step of the way to make sure the conferral of these legal benefits comports with Congress's intent in the Act and works to encourage a more secure country.

31. Some people contend, based on a review of SAFETY Act designations to date, that DHS is applying the SAFETY Act more broadly than the law allows by granting liability protections to companies or entities providing broad services, at times with broad purposes (e.g., security services at sporting facilities). Do you believe that the Act has been implemented in a manner consistent with its original purpose?

Although I understand the purpose of the SAFETY Act, I have no personal experience with this aspect of program implementation. If confirmed, I will review the legal guidance and the Department's interpretation of the SAFETY Act.

Secure and Manage Our Borders

Border Searches

32. The search of electronic devices (e.g., laptops) at the border presents a variety of challenges to federal officials conducting inspections, and has been the subject of recent litigation (*See U.S. v. Cotterman*, 709 F.3d 952 (9th Cir. 2012)). How will you, if confirmed, ensure DHS components, such as Customs and Border Protection, execute border searches in compliance with the law and any potential new legal precedent?

Although the Department is a large organization with multiple components performing many different functions, as noted in previous responses, the legal office of each DHS component works in tandem with and reports to the Office of the General Counsel. If I am confirmed, I intend to reinforce consistency in legal interpretation amongst all DHS components and provide for accountability and oversight over all legal initiatives and advice. In considering novel and developing areas of law, such as the search of electronic devices at the border, this reporting structure allows the Office of the General Counsel, through attorneys at the component or components most affected by a particular development, to provide accurate, timely legal advice so that DHS employees may adapt to legal developments and operate within the confines of existing law without sacrificing mission performance.

With respect to recent developments in the legal doctrine surrounding laptop searches at the border, if confirmed, I would work closely with attorneys at U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and across the Department to ensure that our policies, practices, and procedures adhere to all applicable legal requirements.

Surveillance Technology at the Border

33. Customs and Border Protection personnel use advanced surveillance technology along the border to detect illegal activity. Some have raised legal concerns with the use of these technologies. If confirmed, what legal analysis would you use to ensure that our frontline personnel have the tools they need to work effectively while simultaneously respecting the law and safeguarding the privacy of Americans?

As with any legal analysis, if confirmed, my review of issues concerning the use of advanced surveillance technology along the border will consider all applicable constitutional, statutory, and case law. Additionally, my review would also consider other applicable authorities such as Homeland Security Presidential Directives, Presidential Policy Directives, and Executive Orders. Further, I would examine whether existing Department policies, such as those promulgated by the Privacy Office and the Office for Civil Rights and Civil Liberties, address the use of these technologies in an effort to balance the Department's mission-related needs with its ongoing dedication to safeguarding personal privacy and civil liberties.

Environmental Waivers at the Border

34. The Secure Fence Act provides DHS with a broad authority to waive all "legal requirements" in order to construct fencing along the border. The Senate-passed immigration bill would expand this waiver authority to include patrolling activities on federal lands. What legal analysis would you use in determining whether a legal requirement needs to be waived?

DHS has been provided with the authority to waive all legal requirements that may delay the construction of security barriers along the border. In advising on whether a legal requirement should to be waived, I anticipate the Department would consider the relevant legal requirement and how it relates to the facts presented in the particular situation or whether construction can be expeditiously accomplished without exercising the waiver authority.

Enforce and Administer Our Immigration Laws

Comprehensive Immigration Reform

35. If the Senate-passed comprehensive immigration reform legislation advances, the Department will face daunting implementation challenges across a range of issues and agencies. For instance, the Department would need to undertake multiple large scale acquisitions, rulemakings, and hiring efforts. As General Counsel, you would play a key role in guiding the Department's implementation of the law through your interpretations of its provisions.

    a. Please discuss some of the key challenges you believe the Department would face in implementing comprehensive immigration reform and what you believe the Department would need to do to properly prepare and execute the requirements of the bill.

The passage of comprehensive immigration reform would, as the Committee notes, require the Department to undertake several major acquisitions and significant hiring across multiple components. It also would likely require the construction of new infrastructure and the drafting of numerous rulemakings. All of this would likely need to be accomplished in an accelerated timeframe. The key challenge the Department would likely face is accomplishing all of these key tasks in a timely manner that is consistent with the high legal, ethical, and quality standards to which DHS holds itself. If confirmed as General Counsel, I will be committed to ensuring the Department meets this key challenge.

b. Do you believe the Department would need new or enhanced oversight mechanisms to accompany such an effort and, if so, what role should the Office of General Counsel play in that oversight?

As I understand it, the Department has several mechanisms in place to ensure that all acquisitions, hiring, and other matters are undertaken in compliance with the highest ethical and legal standards. These mechanisms are implemented primarily by the Management Directorate with support from other offices, including the Office of the General Counsel. If confirmed, I will review these mechanisms to ensure they will provide sufficient oversight of the implementation of any immigration reform measures.

c. If confirmed, how do you plan to coordinate the legal interpretations of ICE, USCIS, CBP and other DHS components to ensure successful and consistent implementation of any potential immigration reforms?

As noted in previous responses, at DHS, the chief counsels of the primary immigration components—ICE, USCIS, CBP—report up to the General Counsel in their reporting chain. I understand that the Office of the General Counsel has developed oversight and coordination processes to ensure that legal interpretations are consistent across the Department and with the best reading of the applicable statute.

Prosecutorial Discretion

36. In June 2011, Immigration and Customs Enforcement (ICE) Director John Morton announced new guidance on the use of prosecutorial discretion in immigration matters.

a. What are your views on the use of prosecutorial discretion?

Prosecutorial discretion is employed by all law enforcement organizations. The use of prosecutorial discretion in the immigration context allows immigration enforcement personnel to focus available resources on those individuals posing the greatest threat to national security, public safety, and border security, including criminals, aliens engaged in or suspected of terrorism or espionage, and recent border crossers. This focus is critical during times of limited budgetary resources.

b. As general counsel, how would you endeavor to review policies on the use of prosecutorial discretion across the Department, including as it relates to immigration?

If confirmed, I would provide legal review and guidance on the broad range of operational and policy issues facing the Department as requested by Department and operational component leadership, including prosecutorial discretion.

c. Under what circumstances, if any, would you recommend changes to the 2011 Morton memo, as well as the use of prosecutorial discretion in general at the Department?

If confirmed, I will ensure that all Department policies comply with applicable Constitutional, statutory, and other legal requirements. I understand that the Department's prosecutorial discretion policies, which are supported by Supreme Court precedent, do comply with the applicable legal requirements.

DACA

37. Pursuant to a June 15, 2012, memorandum issued by the Secretary of the Department of Homeland Security, U.S. Citizenship and Immigration Services began the Deferred Action for Childhood Arrivals program (DACA) to register young undocumented immigrants meeting certain criteria and give them temporary relief from deportation and work authorization. A USCIS report for August 15, 2013 through June 30, 2013 shows over 550,000 individuals have applied to this program.

a. Do you believe USCIS has the authority to implement this program and, if so, what is the legal basis for that authority?

Yes. The Secretary of Homeland Security is charged under the Immigration and Nationality Act with enforcement of the immigration laws, and may exercise prosecutorial discretion in furtherance of that responsibility. Recognizing that the possible candidates for removal far exceed the Department's removal capacity in any individual year, the Department – just like any other law enforcement agency – necessarily must prioritize its enforcement efforts. Deferred action allows the Department to defer enforcement against low priority candidates for removal so as to focus the agency's scarce resources on high priority candidates for removal – such as criminal aliens and aliens who pose threats to public safety or national security. The Executive Branch's use of prosecutorial discretion in the immigration context has been ratified several times by the U.S. Supreme Court, including as recently as last year.

b. What do you believe have been the primary administrative and legal challenges, if any, in implementing this program to date?

I believe that the Department has successfully met several administrative challenges in implementing this program to date. As I understand it, these challenges, and the successful responses, have included:

- *Developing a new filing process, including new forms and instructions, for individuals requesting deferred action.*
- *Developing a hiring plan to meet the new workload.*
- *Developing standard operating procedures and new training regimens (that include anti-fraud and national security protocols) to ensure consistency in adjudications, adherence to law, and program integrity.*
- *Continuously shifting workloads between different parts of USCIS in a flexible and efficient manner to ensure workable distribution and minimize the creation of backlogs.*
- *Providing effective outreach and information to the public to ensure maximum transparency and public visibility into the process.*

Visa Overstays

38. By some estimates, individuals who come to the United States legally and overstay their visas make up approximately 40 percent of the illegal immigrant population in this country. Current law penalizes those who overstay their visas for six months or more with, among other things, either a 3— or 10—year ban from admission into the United States after their removal or voluntary departure from the United States. Yet, an April 2011 Government Accountability Office (GAO) report suggested that there are limited enforcement resources for visa overstays. In addition, those who overstay their visa may not fit into one of the priority categories identified in the June 2011 memo by then Director Morton on prosecutorial discretion.

    a. Do you believe it is important for those who overstay the terms of their visas to be held accountable for those violations? Why or why not?

Yes, it is important for those who overstay their visas to be held accountable. The integrity of our immigration system relies on compliance. As with all immigration enforcement matters, enforcement against visa overstays must be done in a smart manner, which focuses first on overstays that threaten national security and public safety.

    b. How should ICE approach its legal responsibilities with respect to those who overstay their visas and the cross cutting issues of prosecutorial discretion identified in the Morton memo?

As with all immigration enforcement matters, the resources devoted to visa overstays must be used in a smart and common sense way, and focus first on overstays that threaten national security and public safety.

EB-5 Investor Visa Program

39. United States Citizenship and Immigration Services (USCIS) recently provided committee staff with a briefing on the Fifth Preference Employment-Based (EB-5) visa program. During the briefing, USCIS informed committee staff that, should an applicant for a regional center also be under investigation for other illegal activity, such as money

laundering or fraud, USCIS does not have sufficient authority to deny the application based on that investigation.

a. What is your understanding of the current legal authority USCIS has to deny applications under the EB-5 visa program?

As I understand it, USCIS has the authority to deny a regional center application and terminate a regional center's designation for participation in the Immigrant Investor Program when a regional center applicant fails to demonstrate that the regional center will promote economic growth.

b. Do you believe this legal authority provides USCIS sufficient bases to deny EB-5 applications to applicants who may be under investigation? Why or why not?

As I understand it, USCIS has statutory authority under some immigration programs to deny cases in the agency's discretion, but under the EB-5 statute, denials are generally limited to instances in which the applicant cannot show that their projects will stimulate the economy and job creation. However, per my understanding, the law is unclear as to how USCIS should handle cases in which a regional center applicant may be the subject of an investigation. If confirmed, I intend to review whether additional denial authority is necessary and, if so, what the extent of that authority should be.

c. In the Senate-passed comprehensive immigration reform bill (S. 744), bill sponsors included language that would potentially address this issue by giving USCIS broader authority to deny an application. However, if S. 744 fails to pass, what action, if any, can USCIS take under its regulatory authority to ensure it has the ability to appropriately deny EB-5 applications associated with criminal activity or open investigations?

As I understand it, USCIS has taken a range of measures to enhance its ability to deny EB-5 applications, using its own administrative authority under existing law. If confirmed, I intend to confer with USCIS to see what other measures, if any, it can take under existing law to further enhance these powers. Moreover, I would make our legislative attorneys fully available to assist in any legislative efforts along these lines.

Safeguard and Secure Cyberspace

40. Please describe what you view the limits of DHS's statutory authority for cyber security to be. What authorities do you believe the Department needs to effectively and efficiently carry out its cybersecurity mission?

I understand that DHS has broad statutory authority under Title II of the Homeland Security Act to work closely with Federal and nonfederal stakeholders to protect U.S. critical infrastructure and to enhance the cybersecurity of critical information systems. This statutory authority is supplemented by an Executive Order, Presidential directives, and Office of Management and Budget memoranda, among other authorities.

These authorities provide a legal footing for DHS to meet the growing challenge faced by the Nation in cyber and carry out its cybersecurity mission. However, DHS statutory authorities must keep pace with evolving technologies and critical infrastructure's growing reliance on cyberspace.

If confirmed, I will ensure that the Office of the General Counsel works with the department's cybersecurity officials to enable DHS to execute its cybersecurity mission in accordance with, and to the fullest extent of, its legal authorities. I will also work with departmental and congressional officials to assist in our efforts to have DHS authorities keep pace with the evolving cyber landscape and threat to the homeland.

41. Bureaucracy within the Department and between partner agencies can be a major hindrance to accomplishing the cybersecurity mission in a timely fashion. For example, for cyber threat information to be most useful, it must be timely and actionable. However, problems with declassification at some federal agencies and the processing of clearances can slow the sharing of such information.

    a. How can the Office of General Counsel help overcome these challenges and ensure timely action?

If confirmed, I will ensure that the Office of the General Counsel works with departmental officials by providing legal support to declassify cyber threat information where appropriate and that security clearances are processed in accordance with applicable legal requirements. Legal assistance must be timely to be effective, and if confirmed, I would strive to ensure that legal support in areas such as this is provided in a timely manner.

    b. How do you plan to work with DHS and other agencies on these issues?

If confirmed, I will work closely with departmental officials responsible for cybersecurity as well as classification and security clearance issues to understand whether potential legal concerns could be slowing the sharing of cybersecurity information. To the extent that there are any such issues and they raise authorities or equities outside of DHS, I will work with colleagues at other departments and agencies to reach resolution in a way that recognizes the real and growing cyber threat to critical infrastructure as well as the need to protect classified information.

42. If confirmed as General Counsel, do you intend to review DHS's current cyber security operations – including the Einstein program – to ensure they comply with existing laws, including privacy and civil liberties laws? If so, how would you go about conducting this review? What procedures would you put in place to monitor these operations going forward to ensure that they remain compliant with existing laws, including laws that limit domestic intelligence activity?

I look forward to learning more about the full range of DHS cyber security operations. Certainly my greatest priority as General Counsel will be ensuring that all DHS programs, including EINSTEIN and other cybersecurity programs, operate in compliance with

applicable laws. I understand that the Office of Legal Counsel within the Department of Justice has opined on this program. If confirmed, I will work with the OGC staff to ensure that departmental cybersecurity operations are appropriately reviewed and carried out legally and in compliance with applicable privacy and civil liberties laws and policies.

I understand that there is a public Privacy Impact Assessment in place for the EINSTEIN program, notifying the public of the steps the Department has taken to mitigate privacy risks. I intend to forge a close working relationship with the Chief Privacy Officer to address privacy matters, including privacy issues related to the Department's cybersecurity efforts.

Ensure Resilience to Disasters

43. What is your view of the Robert T. Stafford Disaster Relief and Emergency Assistance Act's strengths and weaknesses as a statutory framework for disaster assistance?

The Stafford Act is a flexible authority. If confirmed I plan to work closely with the Secretary, the Deputy Secretary, the Administrator of FEMA, and other appropriate senior DHS leadership and will review the existing legal authorities relevant to emergency management, as necessary. Until I can have further discussions with relevant staff, it would be premature for me to offer any opinions or make any recommendations regarding the strengths and weaknesses of such legal authorities. That said, I recognize the importance of clear roles, responsibilities, and lines of authority in this important area.

44. Do you believe FEMA's current regulations and policies support the basic purpose of the Act and mission of the federal government in terms of supporting state and local response and recovery?

As noted above, until I have an opportunity to study these issues more in depth, it would be premature for me to offer any opinions regarding current regulations and policies.

45. One problem after Hurricane Katrina was the high rate of improper payments to individuals under FEMA's Individual and Households Assistance Program. FEMA has since taken many steps to reduce the rate of improper payments in this program. Do you believe DHS and FEMA have the appropriate legal and statutory mechanisms in place to continue to address waste, fraud, and abuse in disaster assistance programs?

It is my understanding that FEMA has implemented multiple system and operational enhancements and lessons learned from the 2005 Gulf Coast disasters to provide prompt service while minimizing the risk of improper payments. It is also my understanding that the Sandy Recovery and Improvement Act of 2013 provided several million dollars for the DHS OIG. If confirmed, I will look into these authorities and support officials at FEMA and the Department of Justice's Criminal and Civil Frauds Sections as they continue to work to reduce this number further.

V. Relations with Congress

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

Yes.

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

Yes.

VI. Assistance

48. Are these answers your own? Have you consulted with DHS or any interested parties? If so, please indicate the individuals or entities with whom you have consulted, and the nature of the assistance they have provided.

The answers are my own. I have consulted with DHS personnel to inquire as to factual or historical information required to provide responses to certain questions. I am responsible for the content of all responses.

I, Stevan E. Bunnell, hereby state that I have read the foregoing Pre-hearing Questions and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

Stevan E. Bunnell
(Signature)

This 12th day of September, 2013

Subscribed and sworn to before me this 12th day of September 2013
Signature of Notary Public
Notary Public, District of Columbia
My commission expires on June 14, 2014

Post-Hearing Questions for the Record
Submitted to Mr. Stevan E. Bunnell
From Senator Tom Coburn

Nominations Hearing on Mr. Stevan E. Bunnell
To be General Counsel,
U.S. Department of Homeland Security
September 18, 2013

1. **Rule of Law**: What role do you believe the rule of law should play generally in our nation and specifically in the execution of your duties as General Counsel at the Department of Homeland Security?

I believe that one of the great and fundamental strengths of our nation is that we are governed by the rule of law, and not by the whim of individual leaders, and also that the laws that govern us are enacted by the people's democratically elected representatives. Although all employees of the Department of Homeland Security have a personal obligation to follow the law, as the chief legal officer of the Department, the General Counsel has a special leadership responsibility to ensure that the Department as a whole -- including the Secretary -- complies with all applicable Constitutional, statutory, and other legal authorities.

2. **Priorities**: What do you expect your initial priorities will be for the Office of General Counsel, should you be confirmed?

If I am fortunate enough to be confirmed, I expect my overarching initial priority will be to ensure that OGC's priorities are aligned with the core missions of the Department, including the paramount priority of preventing terrorist attacks on America. In furtherance of those OGC priorities, I will make it a top early priority to learn as much as possible about key operational missions and how OGC is performing in support of them, and to use what I learn to help establish more specific management and legal policy priorities and action plans. As part of that process I expect to consult extensively with the Acting Secretary and other senior leadership about their priorities for OGC, but I also expect to spend my first few months intensively visiting with a wide array of key OGC stakeholders, including front line employees, asking questions and listening a lot.

   a. Do you anticipate making ***independent*** decisions regarding whether to review certain policies, such as prosecutorial discretion, even if the Department leadership may not affirmatively request or prioritize such a review? Why or why not?

As part of being mission-oriented, if I am confirmed, I will do my best to be responsive to any concerns or suggestions Department leadership may have about the manner in which OGC is supporting key missions. But the duty of the General Counsel is to the overall interests of the Department and the United States, including adherence to the rule of law.

In keeping with that ultimate duty, I would not hesitate to independently undertake a review of a policy or practice that I believed may raise legal issues, regardless of whether I had been asked to do so by Department leadership.

3. **Coordinating the Department's Legal Positions**: In response to your pre-hearing questionnaire, you discussed the importance of consistency of legal positions across the Department. You stated it is "imperative that legal interpretations are applied consistently and communicated across the Department," and you would review the current process in place "to develop and communicate legal positions" within the Department.

    a. Given your experience managing offices, both in your current private law practice and at the D.C. U.S. Attorney's Office, are there any general guidelines you have used in the past to ensure such consistency and would they be applicable to the Office of the General Counsel?

In my experience managing lawyers in private practice and at the DC U.S. Attorney's Office, maintaining consistency on important legal positions and organizational policies can often best be achieved through a combination of reinforcing methods, including a clear and widely disseminated announcement and explanation of the particular legal position and its importance, either through a formal memo or email communication, followed by discussion at staff and other internal meetings. Important legal policies also need to be memorialized in a place where they are readily accessible to all relevant employees (e.g., an internal website or policy manual), integrated into training programs, and most importantly, explicitly and consistently followed by supervisors in the course of regular operations. Finally, it is important to ensure that consistent compliance with Departmental policies and legal positions is an element of attorney and other employee performance evaluations.

4. **Congressional Oversight and Cooperation**: It was apparent in your responses to the pre-hearing questionnaire, in your staff interview, and in your hearing that you clearly value congressional oversight and the important role it plays in holding agencies accountable. I agree that agencies should work with Congress to ensure taxpayer dollars are properly allocated, and I often make oversight requests of the Department of Homeland Security (DHS) for information on a variety of issues. As general counsel, you will be responsible for timely and accurate responses to these inquiries.

    a. During your service as Counsel to the Assistant Attorney General for the Criminal Division at the Justice Department, you stated part of your responsibilities included handling matters involving congressional oversight requests. How will your experience in that position inform your approach to congressional requests for information from DHS?

I had a diverse and evolving set of responsibilities during my time (1999 to 2002) as a Counsel to the Assistant Attorney General for the Criminal Division at the Department of Justice. On those occasions when I was asked to assist with congressional oversight requests, most of my work involved helping to manage the timely collection, review, and production of Criminal Division documents requested by congressional committees.

Although it was not my role to interact directly with Members of Congress or their staff on oversight requests -- that was primarily the role of the Justice Department's Office of Legislative Affairs -- I observed the critical value of good faith communication between DOJ and oversight committees, and if confirmed I would endeavor to assist the Department of Homeland Security in maintaining robust communications with Congress.

b. Can you provide any examples from your time in this position where you advised the Assistant Attorney General to ***withhold*** information from Congress? Please explain your general approach to reaching such a conclusion.

As noted above, my involvement in congressional oversight requests when I worked in the Assistant Attorney General's office was focused on making sure that requested documents were collected and produced in a timely manner.

In my role within the Criminal Division, I occasionally reviewed documents prior to their being produced to Congress to make sure that certain established categories of protected or restricted information were not produced, or not produced in a way that would violate legal requirements, or in a way that could compromise critical national security, law enforcement, or privacy interests. For example, documents within the Criminal Division frequently contained information covered by the Grand Jury secrecy requirements of Federal Rule of Criminal Procedure 6(e), which makes it a potential crime for a federal prosecutor to disclose information relating to matters occurring before a federal grand jury. One of my responsibilities was to make sure that the Assistant Attorney General for the Criminal Division, or others, did not violate Rule 6(e) in the course of providing documents or information to Congress. I also recall situations where Title III wiretap information needed to be redacted from productions so as to comply with the statutory legal protections that apply to that information. Information about classified programs, pending law enforcement investigations, sealed cases, or sensitive personal information (e.g., witness social security numbers, home phone numbers, tax return information, health/medical information) are other examples of types of information sometimes encompassed by congressional requests that I would occasionally identify for redaction or for a restricted disclosure protocol/accommodation.

5. Under the employment-based immigrant investor visa program (EB-5), "regional centers" are business entities in which EB-5 investor applicants contribute a minimum of $500,000, which the regional center pools and invests in new businesses that are supposed to create ten jobs per applicant. In an August briefing to congressional staff, U.S. Citizenship and Immigration Services (USCIS) officials told us they could not shut down a regional center based on fraud or national security concerns. That is, even if they are worried a regional center is committing crimes or helping spies or terrorists enter the United States, they cannot shut it down.

In your questionnaire, you stated USCIS had the authority to deny a regional center application "when a regional center applicant fails to demonstrate that the regional center will promote economic growth."

c. Are there any other circumstances under which you believe USCIS has authority to deny a regional center application or investor application? Why or why not?

As I noted at my confirmation hearing, my knowledge of the EB-5 program is very limited and general. However, I understand that USCIS has the authority to deny a regional center application or investor petition if the applicant or petitioner does not satisfy the applicable statutory and regulatory eligibility requirements. Regional center applicants and immigrant investor petitioners bear the burden of showing eligibility by a preponderance of the evidence, and a finding of fraud will impact the credibility and probative value of evidence and statements.

d. Even if USCIS only has the authority to deny these applications based on failure to demonstrate economic growth, do you believe USCIS ***should*** be able to deny applications on any other bases, such as the existence of an open investigation, findings of fraud, national security concerns or financial crimes? Why or why not?

Yes, based on my limited knowledge of the program, I believe USCIS should have the authority to deny applications on other bases. Should I be confirmed, I would make it a priority upon arriving at DHS to learn about these issues and see what I could do to help increase the security of the EB-5 program.

e. According to the Congressional Research Service (CRS), statutory and regulatory requirements for the EB-5 investor visa program establish eligibility requirements, but do not appear to explicitly outline how to handle fraud. However, CRS suggests derogatory information, such as an open fraud investigation, discovered during the two-year conditional phase of the EB-5 based immigrant status should result in termination of such status. Do you agree?

Unfortunately, my level of knowledge of this program, its history and its authority does not permit me to provide an authoritative answer to this question. I am aware, however, that not all EB-5 related applications, including regional center applications, confer a visa status. Regardless, if confirmed, I would be happy to

review this issue and the Department's legal analysis in this area. Certainly, if there is more USCIS can be doing to increase the security of the program under its existing authorities, it would seem it should.

f. Current immigration law makes inadmissible an alien who fraudulently or through willfully misrepresenting a material fact, seeks or has obtained a visa or other immigration benefit (8 USC § 1182(a)(6)(C)).

- Do you believe fraud in the EB-5 application process equates to such misrepresentation? Why or why not?

Again, I do not believe that I have sufficient knowledge of this program yet to provide an authoritative response. However, I certainly agree that statutory authorities should be utilized where possible in the service of safeguarding against fraud and protecting national security. As noted, not all EB-5-related applications confer admissibility on an alien. For example, my understanding is that a regional center application merely seeks the approval of that regional center so that it can foster investment by multiple individuals; admissibility is not granted upon its approval.

- If yes, regardless of whether the current EB-5 statute explicitly states the program's applications should be denied due to the existence of fraud, do you believe USCIS should deny EB-5 applications on the basis of fraud merely to comply with existing immigration law? Why or why not?

Yes, I believe that every existing authority to deny EB-5 applications on the basis of substantiated fraud should be exercised to the fullest extent the law permits. Any applicant who attempts to defraud the United States should not receive the benefits conferred by the EB-5 program.

6. **Visa Overstays and Prosecutorial Discretion**: In your pre-hearing questionnaire, we asked you about the issue of visa overstays and how Immigration and Customs Enforcement (ICE) should approach its legal responsibilities with respect to those who overstay their visas and the cross cutting issues of prosecutorial discretion identified in the June 2011 memo authored by then-Director John Morton. You stated resources in this area "must be used in a smart and common sense way, and focus first on overstays that threaten national security and public safety."

In an April 2011 report (GAO-11-411), the Government Accountability Office (GAO) noted "strengthening prioritization and assessment of overstay efforts could improve enforcement," and recommended improving information sharing "in support of efforts to identify and take enforcement action against overstays." In March 2012, before the Senate Judiciary Committee, Subcommittee on Immigration, Refugees, and Border Security, GAO testified that the Department of Homeland Security (DHS) should take further steps "to mitigate risks in the Visa Waiver Program," particularly security risks.

How would you reconcile the need for DHS to take appropriate enforcement action to address the problems and risks identified by GAO with the Morton memo discouraging removal or prosecution of certain types of aliens, which may include those who have overstayed their visas?

It is important for visa overstays to be held accountable. As with all immigration enforcement matters, enforcement against visa overstays must be conducted in a common sense and effective manner that prioritizes those overstays who pose a danger to our nation or our communities. As I understand it, DHS has taken important steps to enhance its visa overstay enforcement efforts, by developing a fully-functioning entry/exit system that tracks and identifies overstays. I understand the Department is now able, on a daily basis, to identify and target for enforcement action those who have overstayed their period of admission and who represent a public safety and/or national security threat.. This targeting has been made possible based on improved information sharing between various DHS databases. These efforts, based on my understanding, respond to many of the recommendations made by GAO. However, if I were to conclude, after being confirmed, that the Department's actions regarding visa overstays did not comport with the law, I would not hesitate to take action to address that situation.

7. **Deferred Action for Childhood Arrivals**: In your pre-hearing questionnaire, you noted the Department of Homeland Security (DHS) may use prosecutorial discretion to administer the Deferred Action for Childhood Arrivals program (DACA). As of August 31st, U.S. Citizenship and Immigration Services (USCIS) received 588,725 DACA requests. Of these requests, 455,455 were approved; 21,162 were rejected; and 9,578 were denied. No doubt the program will continue to process thousands of applications for aliens with a variety of backgrounds.

    g. Do you believe there should be any changes to the DACA program to reduce the potential for fraud?

    With my current level of knowledge regarding the DACA program, I am not aware of any deficiencies in the DACA program regarding the potential for fraud. However, if I were to conclude, after being confirmed, that the Department's actions regarding the potential for fraud in the DACA program required changes, I would not hesitate to take action to address that situation.

    h. If not, how do you believe USCIS procedures have been effective in preventing fraud and other national security risks in the DACA program to-date? Please provide examples.

    It is my understanding that, in developing the DACA process, USCIS adopted several measures to combat fraud and protect national security and public safety, and that these measures have proven effective. These measures, as I understand it, include biometric capture and full vetting of each requestor; extensive

collaboration with federal, state and local enforcement authorities; development of an interview process based on both random sampling and fact-based targeting to detect and deter fraud; development of an internal publication on fraud trends in the program based on real-time collection of information from the field; and publication of materials making clear that those seeking to defraud USCIS will be treated as enforcement priorities subject to removal action and criminal prosecution to the fullest extent of the law. These measures build upon the training received by the career officials, including fraud and national security experts, who handle DACA cases.

i. How would you address the tension between the need to uphold the rule of law and the flexibility of the DACA program that may allow for lawful status to be granted to aliens with questionable criminal histories and those who may have violated current immigration law?

As a former prosecutor, I understand the DACA process to be an exercise of the Department's prosecutorial discretion. Similar to prosecutorial discretion in other contexts, it seems to me the use of prosecutorial discretion in the immigration context allows immigration enforcement personnel to focus available resources on those individuals posing the greatest threat to national security, public safety, and border security. It's also noteworthy that USCIS has stated that deferred action does not confer lawful status upon an individual. It merely defers any enforcement action.

8. **Whether the Law Requires DHS to Provide Congressionally-Mandated Reports to HSGAC**: A key provision of the Department of Homeland Security (DHS) Appropriations Act of 2013 requires the Department to provide this committee with copies of reports sent to the House and Senate Appropriations Committees. Yet some components in DHS have informed my staff they interpret this section to cover only those reports signed by the Secretary, excluding any reports issued to the Appropriations Committees by those underneath him like the Deputy Secretary and heads of the components. I am especially troubled by this interpretation of that provision given that many, if not most, Congressionally-mandated reports are signed by someone other than the Secretary and would be exempt from this provision under that interpretation.

"SEC. 574. Fourteen days after the Secretary of Homeland Security submits a report required under this division to the Committees on Appropriations of the Senate and the House of Representatives, the Secretary shall submit a copy of that report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives."

a. Do you believe Sec. 574 includes reports signed by other leadership in DHS who report to the Secretary, as well as those reports signed by the Secretary?

It appears clear from the provided language that section 574 applies to reports that the Secretary must submit. As a general matter, it seems that congressional committees with jurisdiction should have access to reports that Congress has instructed the Department to write. I am not familiar with the past history and practice associated with the subject of this provision, but would review the Department's interpretation of this provision if confirmed.

Post-Hearing Question for the Record
Submitted to Stevan Bunnell
From Senator Kelly Ayotte

"Nominations Hearing"
September 18, 2013

(1) In your opinion, what are the most serious or imminent threats to the homeland that we face today? In other words, what must you be prepared for upon confirmation, and how are you prepared to face those threats?

My current understanding of the serious and imminent threats facing our country is based on what I have read or heard in the public domain -- largely a product of what has been reported in the popular media. I know from my prior experience in the Criminal Division of the Justice Department, where I had regular access to classified intelligence reporting on domestic and international terrorism threats, that there are many threats, that they are constantly evolving, and that they are rarely completely or accurately reported in the popular media. Accordingly, I recognize that any opinion I currently have about the most serious and imminent threats we face is probably based on incomplete information. Having said that, I am personally most concerned about catastrophic threats -- e.g., attacks akin to the attacks of September 11, 2001; the use of nuclear, radiological, biological, or chemical weapons; and increasingly, the risk of a major cyber attack, either state-sponsored or one initiated by a terrorist group.

If I am fortunate enough to be confirmed, two of the top priorities I will have when I start are: (1) to get a full intelligence briefing on the most serious and imminent threats facing us; and (2) to ensure that the Office of the General Counsel is working closely with Department officials and components as they continue to develop and revise contingency plans for responding to different types of threats.

Hearing on the Nomination of:

Suzanne E. Spaulding
To be Under Secretary of the
United States Department of Homeland Security

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

September 18, 2013
342 Dirksen Senate Office Building

Chairman Carper, Ranking Member Coburn, and Members of the Committee,

I am honored that the President has nominated me to serve as Under Secretary for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security (DHS). DHS, and NPPD in particular, are at the forefront of the national imperative to strengthen the security and resilience of the critical infrastructure, cyber and physical, that sustains our way of life. As Acting Under Secretary of NPPD, and before that as Deputy Under Secretary, I have been privileged to work with outstanding homeland security professionals, in and outside of government, committed to the DHS mission of safeguarding the Nation.

My father, a Marine officer, and my mother, a Marine, teacher, and later Hill staffer, both instilled in me the importance of serving one's country. I took this lesson to heart and began working in government on national security issues in 1983. Though my service has been different from my parents', I have developed a deep appreciation not only for the men and women who serve our country in uniform, but also for the civilian public servants who toil each and every day to protect the Nation from myriad threats. It has been an honor to work with these public servants in both the legislative and executive branches, and I look forward to continuing that service, should I be confirmed by the Senate.

I have spent over 25 years working on national and homeland security issues at both ends of Pennsylvania Avenue, on both sides of the Capitol, and on both sides of the aisle. My work on Capitol Hill, including on both the Senate and House intelligence committees, and in the general counsel's office at the Central Intelligence Agency (CIA) focused on protecting the nation from emerging threats. In addition, I worked on several commissions focused on homeland and national security, including as Executive Director of the National Commission on Terrorism and as the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction.

Like many others in government, my work on these issues took on new meaning after the September 11 attacks. The changing threat landscape meant that the Nation and government, collectively, had to prepare for new threats. As part of these efforts, I co-founded the American Bar Association's Cybersecurity Legal Task Force and was appointed by Virginia Governor Mark Warner to the Secure Commonwealth Panel, established to advise the governor and the

legislature regarding preparedness issues in the commonwealth of Virginia. My work on infrastructure protection and with State and local governments has given me a unique perspective on the central roles that cooperation and partnership play in NPPD's mission.

An important principle that underlies our work at DHS is that effective homeland security requires close collaboration with the private sector and other stakeholders, and across party lines. I have a long history of working for and with both Republicans and Democrats and I am committed to forging meaningful partnerships that transcend political affiliation. In addition, having served as an attorney in the private sector representing many owners and operators of the Nation's critical infrastructure, including as Security Counsel for the Business Roundtable, I am attuned to the concerns of many of our private sector partners. At DHS, I have increased our engagement with the private sector and other stakeholders and will continue to ensure that transparency and collaboration are guiding principles for NPPD.

Since I joined DHS as NPPD Deputy Under Secretary in 2011, I have focused on improving management processes and enhancing efficiencies by better integrating our cybersecurity, physical infrastructure protection, including federal facilities, and biometric activities. NPPD has improved its operational and management processes through various ongoing efforts, including co-location of its field forces, streamlining cross-component consequence analysis, and combining our operations centers. These efforts are critically important to the health of the organization and, if confirmed, I will continue that work in partnership with the Congress.

Though I have learned quite a bit serving with the hardworking men and women at NPPD, several important lessons stand out. First, NPPD must continue to strengthen its relationships with its government and private sector partners. The increasing interdependency between physical and cyber infrastructure and across various sectors, requires true partnerships based on trust, mutual understanding of roles and responsibilities stemming from comparative advantages, and transparency. I hope to continue building those relationships if I am confirmed. Second, privacy and transparency are fundamental pillars that underlie NPPD's mission. DHS and NPPD both have Chief Privacy Officers that oversee programs and operations to ensure that everything we do takes into account the privacy and civil liberties of all Americans. In addition, we publish detailed privacy impact assessments about our programs on the Department's website. I pledge

to continue this important work and strive towards the goals of protecting privacy and increasing transparency if I am confirmed. Finally, effective management dictates that we increase the efficiency of our operations and leverage our unique capabilities across physical and cyber infrastructure. As Deputy Under Secretary of NPPD, I oversaw the implementation of numerous management and program reforms in areas ranging from the Chemical Facility Anti-Terrorism Standards (CFATS) program to the co-location of our field forces. In addition, the work NPPD is doing to implement continuous diagnostics and mitigation (CDM) technology across the government and provide a joint assessment capability to our partners will help save money and increase efficiencies, and leverage tools across components.

Though events can often influence priorities, there are important initiatives at NPPD that I am eager to advance if confirmed. The CFATS program has steadily improved since I joined the Department as Deputy Under Secretary. While we implemented significant programmatic and management reforms to improve the program, there is still much to be done. I pledge to continue the reforms we have instituted and work to make CFATS an efficient and effective chemical facilities security program.

The rapidly growing connection between physical and cyber infrastructure requires that we think about infrastructure protection holistically and understand the potential consequences across multiple critical infrastructure sectors. If confirmed, I plan to continue efforts underway to better integrate the cyber and physical domains and focus our resources on understanding the consequences of an attack and measures to mitigate those consequences.

Building on the good work that NPPD is already doing, I pledge to strengthen relationships with our government partners and the private sector. Our Nation's security depends on strong public-private relationships. One of NPPD's most important missions is to build robust partnerships that will allow us to better serve the American people by increasing the security and resilience of the critical infrastructure upon which they rely.

Finally, none of these mission objectives can be accomplished without a capable and committed workforce. I will continue to make it a priority to empower the dedicated men and women at NPPD with a clear sense of mission and the tools they need to advance our important mission.

In addition, we must continue to recruit the best and the brightest to build our capabilities to meet the challenges we face.

I have dedicated much of my career to public service, a commitment to protecting and preserving the American ways of life, and an understanding that success requires close collaboration among all levels of government, with the private sector, and with the Congress. I have tried to incorporate these core principles into my work at DHS. I pledge to continue that same commitment, dedication and understanding to the position of Under Secretary if I am confirmed by the United States Senate.

Thank you for the opportunity to appear before you today, and I look forward to answering any questions you may have.

REDACTED

HSGAC BIOGRAPHICAL QUESTIONS FOR EXECUTIVE NOMINEES

1. Basic Biographical Information

Please provide the following information.

Position to Which You Have Been Nominated	
Name of Position	**Date of Nomination**
Under Secretary, National Protection and Programs Directorate, Department of Homeland Security	August 2, 2013

Current Legal Name			
First Name	**Middle Name**	**Last Name**	**Suffix**
Suzanne	Eleanor	Spaulding	

Addresses					
Residential Address (do not include street address)			**Office Address** (include street address)		
[redacted]			Street: 1616 N. Fort Myer Drive		
City: McLean	State: VA	Zip:22101	City: Arlington	State: VA	Zip: 22209

Other Names Used						
First Name	**Middle Name**	**Last Name**	**Suffix**	Check if Maiden Name	**Name Used From** (Month/Year) (Check box if estimate)	**Name Used To** (Month/Year) (Check box if estimate)
					Est ☐	Est ☐
					Est ☐	Est ☐

Birth Year and Place	
Year of Birth (Do not include month and day.)	**Place of Birth**
1957	Camp Lejeune, NC

Marital Status					
Check All That Describe Your Current Situation:					
Never Married	**Married**	Separated	Annulled	Divorced	Widowed
☐	X	☐	☐	☐	☐

Spouse's Name (current spouse only)			
Spouse's First Name	Spouse's Middle Name	Spouse's Last Name	Spouse's Suffix
Gary	David	Slaiman	

Spouse's Other Names Used (current spouse only)						
First Name	Middle Name	Last Name	Suffix	Check if Maiden Name	Name Used From (Month/Year) (Check box if estimate)	Name Used To (Month/Year) (Check box if estimate)
					Est ☐	Est ☐
					Est ☐	Est ☐

Children's Names (if over 18)			
First Name	**Middle Name**	**Last Name**	**Suffix**
Charlotte	Spaulding	Slaiman	
Max	Dylan	Slaiman	

2. Education

List all post-secondary schools attended.

Name of School	**Type of School** (vocational/technical/trade school, college/university/military college, correspondence/distance/extension/online school)	**Date Began School** (month/year) (check box if estimate)	**Date Ended School** (month/year) (check box if estimate) (check "present" box if still in school)	**Degree**	**Date Awarded**
University of Virginia, Bachelor of Arts	College	1974 Est ☐	1978 Est ☐ Present ☐	BA	1978
University of Virginia Law School	Law School	1978 Est ☐	1981 Est ☐ Present ☐	JD	1981
		Est ☐	Est ☐ Present ☐		
		Est ☐	Est ☐ Present ☐		

3. Employment

(A) List all of your employment activities, including unemployment and self-employment. If the employment activity was military duty, list separate employment activity periods to show each change of military duty station. Do not list employment before your 18th birthday unless to provide a minimum of two years of employment history.

Type of Employment (Active Military Duty Station, National Guard/Reserve, USPHS Commissioned Corps, Other Federal employment, State Government (Non-Federal Employment), Self-employment, Unemployment, Federal Contractor, Non-Government Employment (excluding self-employment), Other	Name of Your Employer/ Assigned Duty Station	Most Recent Position Title/Rank	Location (City and State only)	Date Employment Began (month/year) (check box if estimate)	Date Employment Ended (month/year) (check box if estimate) (check "present" box if still employed)
Federal Government Employment	Congressman Jim Johnson (R-CO)	Intern	Washington, D.C.	Summer 1976	1976
Non-Government Employment	Fish Market Restaurant	Bartender	Alexandria, VA	Summer 1978	1978
Non-Government Employment	AAUW- National Coalition on Women and Girls	Intern	Washington, D.C.	Summer 1979	1979
Non-Government Employment	Cooley, Godward, Castro, Huddleston & Tatum	Summer Associate	Washington, D.C.	May 1980	June 1980
Non-Government Employment	Cadwalader, Wickersham & Taft	Summer Associate	Washington, D.C.	July 1980	August 1980
Non-Government Employment	Crowell & Moring	Associate	Washington, D.C	1981 Est ☐	1983 Est ☐
Other Federal employment	U.S. Senator Arlen Specter	Senior Counsel/Legislative Director	Washington, D.C	1983 Est ☐	April1987 Est ☐
Other Federal employment	CIA	Attorney Advisor	McLean, VA	April 1989 Est ☐	March 1995 Est ☐
Other Federal employment	Senate Select Committee on Intelligence	General Counsel	Washington, D.C	March 1995 Est ☐	1997 Est ☐
Other Federal employment	Federal Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass	Executive Director	McLean, VA	1998 Est ☐	July 1999 Est ☐

	Destruction				
Self-Employment	Mother	Mother	McLean, VA	1999	2000
Other Federal employment	National Commission on Terrorism	Executive Director	Washingt on, D.C	Feb 2000 Est ☐	June 2000 Est ☐
Self-Employment	Consultant (during this time Spaulding served as a consultant to the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction)	Consultant	McLean, VA	June 2000	Aug 2003
Other Federal employment	U.S House of Representatives	Minority Staff Director, House Permanent Select Committee on Intelligence	Washingt on, D.C	Sept 2003 Est ☐	Sept 2004 Est ☐
Self-Employment	Consultant (during this time, Spaulding served as a consultant to the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction)	Consultant	McLean, VA	Aug 2004 Est ☐	Jan 2005 Est ☐
Non-Government Employment	The Harbour Group	Managing Partner	Washingt on, D.C	Jan 2005 Est ☐	Feb 2006 Est ☐
Non-Government Employment	Bingham McCutchen	Consultant and Of Counsel	Washingt on, D.C	Mar 2006 Est ☐	Oct 2011 Est ☐
Other Federal employment	Department of Homeland Security	Deputy Under Secretary	Washingt on, D.C	Oct 2011 Est ☐	May 2013 Est ☐
Other Federal employment	Department of Homeland Security	Acting Under Secretary	Washingt on, D.C	May 2013 Est ☐	Present Est ☐

(B) List any advisory, consultative, honorary or other part-time service or positions with federal, state, or local governments, not listed elsewhere.

Name of Government Entity	Name of Position	Date Service Began	Date Service Ended (month/year) (check box

		(month/year) (check box if estimate)	if estimate) (check "present" box if still serving)
Virginia Secure Commonwealth Panel (State Advisory Panel)	Member	Est 2002 □	Est Present 2004□ □
ODNI Counterintelligence Review panel	Consultant	Est □x April 2009	Est Present □x □ July 2009
		Est □	Est Present □ □

4. Potential Conflict of Interest

(A) 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 entered into with the Department's Designated Agency Ethics Official that will be provided to this Committee. I am not aware of any other potential conflicts of interest.

(B) 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 was a registered lobbyist from 2005-2008. In addition, I have testified on a number of legislative proposals (noted in question 8(B) below) and organized and/or signed on to statements regarding national security issues with others, including other former national security officials. Finally, I have often spoken publically or met with executive and legislative branch officials to help inform discussion and debate on issues related to legislation or public policy related to national security.

5. Honors and Awards

List all scholarships, fellowships, honorary degrees, civilian service citations, military medals, academic or professional honors, honorary society memberships and any other special recognition for outstanding service or achievement.

Senior Fellow, Homeland Security Policy Institute, George Washington University (2008, 2011)
Several performance awards at CIA.

6. Memberships

List all memberships that you have held in professional, social, business, fraternal, scholarly, civic, or charitable organizations in the last 10 years.

Unless relevant to your nomination, you do NOT need to include memberships in charitable organizations available to the public as a result of a tax deductible donation of $1,000 or less, Parent-Teacher Associations or other organizations connected to schools attended by your children, athletic clubs or teams, automobile support organizations (such as AAA), discounts clubs (such as Groupon or Sam's Club), or affinity memberships/consumer clubs (such as frequent flyer memberships).

Name of Organization	Dates of Your Membership (You may approximate.)	Position(s) Held
D.C. Bar	1981-Present	Member
Bipartisan Security Group	1999-2004	Member
CSIS Chemical, Biological, Radiological and Nuclear Terrorism Task Force	1999-2001	Task Force Member
CSIS Cyber Threats of the Future Task Force	1999-2001	Task Force Member
American Foreign Intelligence Officers	2008-2011	Board Member
American Bar Association, Standing Committee on Law and National Security	2001-2011	Chair, Alumni Committee Chair, Special Advisor
Aspen Institute Homeland Security Task Force	2011	Task Force Member
Constitution Project	2009-2011	Advisory Board Member
Critical Incidents Analysis Group/UVA School of Medicine	2006-2010	Steering Committee Member
CSIS Transnational Threats Project	2006	Member, Core Advisory Group

CSIS Cybersecurity Commission	2008-2009	Task Force Member
GWU Homeland Security Policy Institute	2008, 2011	Senior Fellow
CSIS Transnational Threats Project	2009	Member, Senior Advisory Group
Intelligence National Security Alliance	2010-2011	Special Advisor
International Security and Biopolicy Institute	2009-2011	Advisory Board Member

7. Political Activity

(A) Have you ever been a candidate for or been elected or appointed to a political office?

No.

Name of Office	Elected/Appointed/ Candidate Only	Year(s) Election Held or Appointment Made	Term of Service (if applicable)

(B) List any offices held in or services rendered to a political party or election committee during the last ten years that you have not listed elsewhere.

Name of Party/Election Committee	Office/Services Rendered	Responsibilities	Dates of Service
Kerry for President	Volunteer	Leafleting; some consultation on national security	9/04-11/04
Obama for President	Volunteer	Leafleting; some consultation on intelligence issues	8/08-11/08

(C) Itemize all individual political contributions of $200 or more that you have made in the past five years to any individual, campaign organization, political party, political action

committee, or similar entity. Please list each individual contribution and not the total amount contributed to the person or entity during the year.

Name of Recipient	Amount	Year of Contribution
Friends of Mark Warner	$1000	2013
Oceans PAC	$250	2013
Barack Obama	$1000	2012
Tom Perriello	$250	2010
Tim Kaine	$250	2012
Tim Kaine	$250	2012
Patrick Leahy	$200	2009
Judith Feder	$250	2008

8. Publications and Speeches

(A) List the titles, publishers and dates of books, articles, reports or other published materials that you have written, including articles published on the Internet. Please provide the Committee with copies of all listed publications. In lieu of hard copies, electronic copies can be provided via e-mail or other digital format.

I have done my best to identify titles, publishers and dates of books, articles, reports or other published materials, including a thorough review of my personal files and searches of publicly available electronic databases. Despite my searches, there may be other materials I have been unable to identify, find, or remember. I have located the following:

Title	Publisher	Date(s) of Publication
"Building Checks and Balances for National Security Policy: The Roles of Congress."	Advance, American Constitution Society for Law and Policy, Vol.2,	Fall 2008

	No.2,	
"Stuck in a September 12 Mindset." Suzanne Spaulding, The Guardian,	Huffington Post http://www.guardian.co.uk/commentisfree/2008/sep/11/september11.usforeignpolicy	September 11, 2008
"Don't Let Terrorists Snatch Victory from the Jaws of Defeat."	Huffington Post http://www.huffingtonpost.com/suzanne-e-spaulding/dont-let-terrorists-snatc_b_566784.html	May 6, 2010
"Don't Rescue the Global Jihad."	Huffington Post http://www.huffingtonpost.com/suzanne-e-spaulding/dont-rescue-the-global-ji_b_867072.html	May 25, 2011
"No More Secrets: Then What?"	Huffington Post http://www.huffingtonpost.com/suzanne-e-spaulding/no-more-secrets-then-what_b_623997.html	June 24, 2010
"Saving the DNI from Extinction."	Huffington Post http://www.huffingtonpost.com/suzanne-e-spaulding/saving-the-dni-from-extin_b_589704.html	May 25, 2010
"Will the Real America Please Stand Up."	Huffington Post http://www.huffingtonpost.com/suzanne-e-spaulding/will-the-real-america-ple_b_707287.html	June 7, 2010
"Yes, a Strong and Resilient Nation Can Absorb a Terrorist Attack."	Huffington Post http://www.huffingtonpost.com/suzanne-e-spaulding/yes-a-strong-and-resilien_b_735623.html	September 22, 2010
"Power Play: Did Bush Roll Past the Legal Stop Signs?"	The Washington Post	December 25, 2005
"The Deutch commission report: An overview."	*The Nonproliferation review.* (12/1999), 6 (4), P. 168.	December 1999
Brief *Amici Curiae* of Former National Security Officials and Counterterrorism Experts in Support of Petitioner, Ali Saleh	http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/08-368.htm	January 2009

Kahlah Al-Marri (Petitioner) v. Daniel Spagone, U.S.N. Commander, Consolidated Naval Brig (Respondent), On Writ of Certiorari to the United States Court of Appeals for the Fourth Circuit. No. 08-369 in the Supreme Court of the United States. By: Suzanne Spaulding, Sabin Willett, Rheba Rutkowski, Catherine Murphy.		
"Legal Framework for Shielding."	*International journal of emergency mental health.* (2002), 4 (4), p. 259.	2002
"Intercepting Lone Wolf Terrorists," Suzanne Spaulding and Michael J. Woods.	*Patriot Debates.* (2005) American Bar Association p. 81	2005
"A National Security Career: Passion, Networking, and a Little Luck."	*Careers in National Security Law* American Bar Association (2008) p. 27	2008
"Homeland Security."	*National Security Law 2nd Edition* (2005) p. 1267	2005
Statement of Former National Security Officials.	http://www.constitutionproject.org/wp-content/uploads/2012/09/318.pdf	September 25, 2006
Statement of Former Government Officials.	http://www.constitutionproject.org/wp-content/uploads/2012/09/302.pdf	February 8, 2006
Letter to Chairman Arlen Specter (R-PA) from the Bipartisan Working Group of Former Government Officials.		June 17, 2005
Civil Liberties in a Post 9/11 World, Appendix E	http://www.rand.org/content/dam/rand/www/external/nsrd/terrpanel/volume_v/volume_v_appendices_only.pdf	December 15, 2001
"Turning Point: Even as Threats Still Loom, US Officials Raise Possibility of Defeating al-Qaida."	ABA Journal Vol. 97 Issue 9, p28-28.	September 2011

"Ideas for America's Future: Core Elements of a New National Security Strategy."	Bialos, Jeffrey P., Koehl, Stuart, Catarious, David M., Spaulding, Suzanne. Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University.	2008
Participant and briefly contributed in "Force Multiplier for Intelligence: Collaborative Open Source Networks." Page 24	Arnaud De Borchgrave, Thomas M. Sanderson, Jacqueline Harned. *CSIS*	July 31, 2007
Criminal Prosecution of Abdulmutallab Best Meets Counterterrorism Objectives, Memo to Interested Parties	Center for National Security Studies	January 27, 2010
A message to Congress from National Security and Terrorism Experts: Blocking the government from bringing any Guantanamo detainees to the U.S. is unnecessary and harmful to our national security	Homeland Security Policy Institute	July 10, 2009
Cyber Threats and Information Security: Meeting the 21st Century Challenge	CSIS http://csis.org/programs/transnational-threats-project/transnational-threats-project-past-task-forces/cyber-threats-	May 1, 2001

(B) List any formal speeches you have delivered during the last five years and provide the Committee with copies of those speeches relevant to the position for which you have been nominated. Include any testimony to Congress or any other legislative or administrative body. These items can be provided electronically via e-mail or other digital format.

Title/Topic	Place/Audience	Date(s) of Speech
Rule of Law	Hearing before the Subcommittee on the Constitution, Committee on the Judiciary, United States Senate	September 16, 2008
Confirmation Hearing on Federal Appointments	Hearing before the Committee on the Judiciary, United States Senate	February 5, February 25, March 10, and April 1, 2009

USA PATRIOT Act	Hearing before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Committee on the Judiciary	September 22, 2009
Reauthorizing the USA PATRIOT Act: Ensuring Liberty	Hearing before the Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, United States Senate	September 23, 2009
Securing America's Safety: Improving the Effectiveness of Antiterrorism Tools and Interagency Communication	Hearing before the Committee on the Judiciary, United States Senate	January 20, 2010
Department of Homeland Security Appropriations for 2013	Hearing before the Subcommittee on Appropriations, House of Representatives	July 26 and September 20, 2012

(C) List all speeches and testimony you have delivered in the past ten years, except for those the text of which you are providing to the Committee.

Title	Place/Audience	Date(s) of Speech
Global (in)security	Young Presidents' Organization	September 3, 2003
Enemy Combatants	American Bar Association Standing Committee on Law and National Security	February 24, 2004
Legal Responses to the Terrorism Threat	American Bar Association	April 13, 2004
Implementation of the USA Patriot Act: Sections of the Act that Address the Foreign Intelligence Surveillance Act	Hearing before the Subcommittee on the Judiciary, House of Representatives	April 26 and April 28, 2005
Continued Oversight of the USA PATRIOT Act	Hearing Before Judiciary Committee, United States Senate	May 10, 2005

Incitement Laws	American Bar Association Standing Committee on Law and National Security	November 4, 2005
Checks and Balances	NYU Center on Law and Security	April 25, 2006
Over-Classification and Pseudo-Classification: Part I, II, and III	Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, House of Representatives	March 22, 2007, April 26, 2007, and June 28, 2007.
Listening for Terrorists: Surveillance Programs? Lessons Learned and the Way Ahead	Heritage Foundation http://www.heritage.org/research/commentary/2007/04/listening-for-terrorists-surveillance-programslessons-learned-and-the-way-ahead	April 2007
Responding to the Inspector General's Findings of Improper Use of National Security Letters by the FBI	Hearing before the Subcommittee on the Judiciary, United States Senate	April 11, 2007
Modernization of the Foreign Intelligence Surveillance Act	Hearing before the Select Committee on Intelligence, United States Senate	May 1, 2007
Participant and briefly contributed in "Force Multiplier for Intelligence: Collaborative Open Source Networks."	Arnaud De Borchgrave, Thomas M. Sanderson, Jacqueline Harned. *CSIS*, p.24	July 31, 2007
Warrantless Surveillance and the Foreign Intelligence Act: The Role of Checks and Balances in Protecting	Hearing before the Committee on the Judiciary, House of Representatives	September 5, 2007

America's Privacy Rights (Part I)		
Strengthening FISA: Does the Protect America Act Protect American's Civil Liberties and Enhance Security?	Hearing before the Committee on the Judiciary, United States Senate	September 25, 2007
Future Surveillance Laws	American Bar Association Standing Committee on Law and National Security	March 3, 2008
FISA Reform	The Duke University Center on Law Ethics, and National Security and the Program in Public Law	April 1-11, 2008
Terrorism Intelligence	American Bar Association	May 6, 2009
Integrating Disciplines: Cybersecurity, Law, and Policy	Georgetown University School of Law	October 1, 2009
Approaches to Accounting for Post-9/11 Counterterrorism Policies and Actions: The Pros and Cons	CSIS	October 8, 2009
Legal Perspective on National Security Law	American Bar Association	November 12, 2009
Is Now the Time for a Domestic Intelligence Agency	Center for Strategic International Studies Global Security Forum	May 14, 2010
Open Source Intelligence	Lexis-Nexis	December 15, 2010
Intelligence Collection and Law Enforcement: New Roles, Challenges	The Brennan Center for Justice at NYU School of Law	March 18, 2011

Living in a September 12 Mindset	Constitution Project	May 12, 2011
Homeland Security and Privacy	Center for Strategic International Studies	September 7, 2011
Panel on The Evolving Terrorist Threat and the Importance of Intelligence to Protect the Homeland	Office of the Director of National Intelligence	September 7, 2011
9/11 10 Years Later: Changes in Surveillance	American Constitution Society	September 8, 2011
Ten years later: insights on al-Qaeda's past & future through captured records	The Johns Hopkins University Center for Advanced Governmental Studies	January 27, 2012
Cybersecurity and the Private Sector	Wells Fargo Clearance Compliance Roundtable	April 12, 2012
Office of the DCI History Collection	George Mason University School of Public Policy	September 13, 2012
Protecting the Infrastructure	American Bar Association Standing Committee on Law and National Security	September 13, 2012
International Right-to-Know Day	American University Washington College of Law	September 28, 2012
Welcoming Remarks	Critical Infrastructure Partnership Advisory Council	October 3, 2012
Cybersecurity Symposium	Securities Industry and Financial Markets Association (SIFMA)	October 3, 2012
Reimagining Critical Infrastructure in a Changing World	American Bar Association Standing Committee on Law and National Security	December 13, 2012

Cybersecurity	Association DC Chapter	22, 2013
The Threat of a Cyber Attack	Georgetown University School of Law	March 13, 2013
Combating Asymmetric Threats: The Interplay of Offense and Defense	CACI International	April 2, 2013
Critical Infrastructure Security and Resilience	George Mason University School of Law	April 2, 2013
Cyber Threats and the EO	American Bar Association Cybersecurity Legal Task Force	April 19, 2013
Interdependence of Physical and Cyber Infrastructure	Canadian Embassy in Washington, D.C.	May 2, 2013
Plan to Reduce Gun Violence Summary and Background	DC Public School's Kick-Off re: the President's Plan to Reduce Gun Violence	May 20, 2013
History of Cyber Critical Infrastructure Protection: 15th Anniversary of Presidential Decision Directive 63 on Critical Infrastructure Protection	The Atlantic Council	May 22, 2013
A Look at the National Protection and Programs Directorate and What to Expect in 2013	ABA Homeland Security Law Institute	June 20, 2013
NPPD: Infrastructure Protection from Nuts & Bolts to Routers	Cyber Fajitas and Margaritas	July 9, 2013
Panel re: Industry's Role in Cybersecurity	Aspen Security Forum	July 19, 2013
Future of CI Risk Management and the	George Washington University	July 25, 2013

NIPP		
Public Private Partnership discussion re: Cybersecurity Executive Order	Building Resilience through Public-Private Partnerships Conference at the American Red Cross Headquarters	July 31, 2013

9. Criminal History

Since (and including) your 18th birthday, has any of the following happened? No

- Have you been issued a summons, citation, or ticket to appear in court in a criminal proceeding against you? (Exclude citations involving traffic infractions where the fine was less than $300 and did not include alcohol or drugs.)
- Have you been arrested by any police officer, sheriff, marshal or any other type of law enforcement official?
- Have you been charged, convicted, or sentenced of a crime in any court?
- Have you been or are you currently on probation or parole?
- Are you currently on trial or awaiting a trial on criminal charges?
- To your knowledge, have you ever been the subject or target of a federal, state or local criminal investigation?

If the answer to any of the questions above is yes, please answer the questions below for each criminal event (citation, arrest, investigation, etc.). If the event was an investigation, where the question below asks for information about the offense, please offer information about the offense under investigation (if known).

A) Date of offense:

   a. Is this an estimate (Yes/No):

B) Description of the specific nature of the offense:

C) Did the offense involve any of the following?
   1) Domestic violence or a crime of violence (such as battery or assault) against your child, dependent, cohabitant, spouse, former spouse, or someone with whom you share a child in common: **Yes / No**
   2) Firearms or explosives: **Yes / No**
   3) Alcohol or drugs: **Yes / No**

D) Location where the offense occurred (city, county, state, zip code, country):

E) Were you arrested, summoned, cited or did you receive a ticket to appear as a result of this offense by any police officer, sheriff, marshal or any other type of law enforcement official: **Yes / No**

1) Name of the law enforcement agency that arrested/cited/summoned you:

2) Location of the law enforcement agency (city, county, state, zip code, country):

F) As a result of this offense were you charged, convicted, currently awaiting trial, and/or ordered to appear in court in a criminal proceeding against you: **Yes / No**

1) If yes, provide the name of the court and the location of the court (city, county, state, zip code, country):

2) If yes, provide all the charges brought against you for this offense, and the outcome of each charged offense (such as found guilty, found not-guilty, charge dropped or "nolle pros," etc). If you were found guilty of or pleaded guilty to a lesser offense, list separately both the original charge and the lesser offense:

3) If no, provide explanation:

G) Were you sentenced as a result of this offense: **Yes / No**

H) Provide a description of the sentence:

I) Were you sentenced to imprisonment for a term exceeding one year: **Yes / No**

J) Were you incarcerated as a result of that sentence for not less than one year: **Yes / No**

K) If the conviction resulted in imprisonment, provide the dates that you actually were incarcerated:

L) If conviction resulted in probation or parole, provide the dates of probation or parole:

M) Are you currently on trial, awaiting a trial, or awaiting sentencing on criminal charges for this offense: **Yes / No**

N) Provide explanation:

10. Civil Litigation and Administrative or Legislative Proceedings

(A) Since (and including) your 18th birthday, have you been a party to any public record civil court action or administrative or legislative proceeding of any kind that resulted in (1) a finding of wrongdoing against you, or (2) a settlement agreement for you, or some other person or entity, to make a payment to settle allegations against you, or for you to take, or refrain from taking, some action. Do NOT include small claims proceedings.

No.

Date Claim/Suit Was Filed or Legislative Proceedings Began	Court Name	Name(s) of Principal Parties Involved in Action/Proceeding	Nature of Action/Proceeding	Results of Action/Proceeding

(B) In addition to those listed above, have you or any business of which you were an officer, director or owner ever been involved as a party of interest in any administrative agency proceeding or civil litigation? 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.

No.

Date Claim/Suit Was Filed	Court Name	Name(s) of Principal Parties Involved in Action/Proceeding	Nature of Action/Proceeding	Results of Action/Proceeding

(C) For responses to the previous question, 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.

11. Breach of Professional Ethics

(A) Have you ever been disciplined or cited for a breach of ethics or unprofessional conduct by, or been the subject of a complaint to, any court, administrative agency, professional association, disciplinary committee, or other professional group? Exclude cases and proceedings already listed.

No.

Name of Agency/Association/ Committee/Group	Date Citation/Disciplinary Action/Complaint Issued/Initiated	Describe Citation/Disciplinary Action/Complaint	Results of Disciplinary Action/Complaint

(B) Have you ever been fired from a job, quit a job after being told you would be fired, left a job by mutual agreement following charges or allegations of misconduct, left a job by mutual agreement following notice of unsatisfactory performance, or received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as violation of a security policy?

No.

12. Tax Compliance

REDACTED

REDACTED

13. Lobbying

In the past ten years, have you registered as a lobbyist? If so, please indicate the state, federal, or local bodies with which you have registered (e.g., House, Senate, California Secretary of State).

Yes, I was registered as a lobbyist from 2005-2008 with the U.S. House of Representatives and the U.S. Senate.

14. Outside Positions

X See OGE Form 278. (If, for your nomination, you have completed an OGE Form 278 Executive Branch Personnel Public Financial Disclosure Report, you may check the box here to complete this section and then proceed to the next section.)

For the preceding ten calendar years and the current calendar year, report any positions held, whether compensated or not. Positions include but are not limited to those of an officer, director, trustee, general partner, proprietor, representative, employee, or consultant of any corporation, firm, partnership, or other business enterprise or any non-profit organization or educational institution. Exclude positions with religious, social, fraternal, or political entities and those solely of an honorary nature.

Name of Organization	Address of Organization	Type of Organization (corporation, firm, partnership, other business enterprise, other non-profit organization, educational institution)	Position Held	Position Held From (month/year)	Position Held To (month/year)

15. Agreements or Arrangements

X See OGE Form 278. (If, for your nomination, you have completed an OGE Form 278 Executive Branch Personnel Public Financial Disclosure Report, you may check the box here to complete this section and then proceed to the next section.)

As of the date of filing your OGE Form 278, report your agreements or arrangements for: (1) continuing participation in an employee benefit plan (e.g. pension, 401k, deferred compensation); (2) continuation of payment by a former employer (including severance payments); (3) leaves of absence; and (4) future employment.

Provide information regarding any agreements or arrangements you have concerning (1) future employment; (2) a leave of absence during your period of Government service; (3) continuation of payments by a former employer other than the United States Government; and (4) continuing participation in an employee welfare or benefit plan maintained by a former employer other than United States Government retirement benefits.

Status and Terms of Any Agreement or Arrangement	Parties	Date (month/year)

16. Additional Financial Data

REDACTED

SIGNATURE AND DATE

I hereby state that I have read the foregoing Statement on Biographical and Financial Information and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

This 21st day of August, 2013

District of Columbia: SS
Subscribed and Sworn to before me,
this 21st day of August, 2013

Notary Public, D.C.
My commission expires 1.31.2017

STUART A. COMMOLLY NOTARY PUBLIC MY COMMISSION EXPIRES 1/31/2017 DISTRICT OF COLUMBIA

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

SEP 10 2013

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

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

We have reviewed the report and have 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,

Don W. Fox
Principal Deputy Director

Enclosures **REDACTED**

September 5, 2013

Joseph Maher
Designated Agency Ethics Official
Department of Homeland Security
Washington, D.C. 20528-0485

Dear Mr. Maher,

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 Directorate, 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.

My spouse and I will divest our interests in the following entities within 90 days of my confirmation (see attached list). With regard to each of these entities, I will not participate personally and substantially in any particular matter that has a direct and predictable effect on the financial interests of the entity until I have divested it, 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).

My spouse is currently a partner with the law firm of Bingham McCutchen, LLP. I will not participate personally and substantially in any particular matter that has a direct and predictable effect on the financial interest of the firm, unless I first obtain a written waiver, pursuant to 18 U.S.C. § 208(b)(1). I also will not participate personally and substantially in any particular matter involving specific parties in which a client of my spouse is a party or represents a party, unless I have been authorized to participate, pursuant to 5 C.F.R. § 2635.502(d). In addition, for the duration of my appointment to the position of Under Secretary for National Protection and Programs Directorate, my spouse has agreed not to communicate with the Department of Homeland Security on behalf of the firm or any client.

I understand that as an appointee I must continue to abide by the Ethics Pledge (Exec. Order No. 13490) that I previously signed and that I will be bound by the requirements and restrictions therein in addition to the commitments I have made in this and any other ethics agreement.

I have been advised that this ethics agreement will be posted publicly, consistent with 5 U.S.C. § 552, on the website of the U.S. Office of Government Ethics with other ethics agreements of Presidential nominees who file public financial disclosure reports.

Sincerely,

Suzanne E. Spaulding

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

Questions from Chairman Senator Carper

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)?

Response: I am honored that the President has nominated me to serve as Under Secretary for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security (DHS). DHS, and NPPD in particular, are at the forefront of protecting the Nation's civilian physical and cyber infrastructure from rapidly evolving threats. As Acting Under Secretary of NPPD, and before that as Deputy Under Secretary, I have been privileged to work with outstanding homeland security professionals, in and outside of government, committed to the DHS mission of safeguarding the Nation. I have dedicated much of my career to public service, a commitment to protecting and preserving the American ways of life, and an understanding that success requires close collaboration among all levels of government, with the private sector, and with the Congress. I have tried to incorporate these core principles into my work at DHS. I pledge to continue that same commitment, dedication and understanding to the position of Under Secretary if I am confirmed by the United States Senate.

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

Response: No.

3. What specific background and experience affirmatively qualifies you to be Under Secretary for NPPD?

Response: My father, a Marine officer, and my mother, a Marine, teacher, and later Hill staffer, both instilled in me the importance of serving one's country. I took this lesson to heart and began working in government on national security issues in 1983. Though my service has been different from my parents, I have developed deep appreciation not only for the men and women who serve our country in uniform, but also for the civilian public servants who toil each and every day to protect the Nation from myriad threats. It has been an honor to work with these public servants in both the legislative and executive branches, and I look forward to continuing that service, should I be confirmed by the Senate.

I have spent over 25 years working on national and homeland security issues at both ends of Pennsylvania Avenue, on both sides of the Capitol, and on both sides of the aisle. My work on Capitol Hill, including on both the Senate and House intelligence committees, and in the general

counsel's office at the Central Intelligence Agency (CIA) focused on protecting the nation from emerging threats. In addition, I served on numerous commissions focused on homeland and national security, including as Staff Director of the National Commission on Terrorism and as a member of the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction.

Like many others in government, my work on these issues took on new meaning after the September 11 attacks. The changing threat landscape meant that the Nation and government, collectively, had to prepare for new threats. As part of these efforts, I co-founded the American Bar Association's Cybersecurity Legal Task Force and was appointed by Virginia Governor Mark Warner to the Secure Commonwealth Panel, established to advise the governor and the legislature regarding preparedness issues in the Commonwealth of Virginia. My work on infrastructure protection and with State and local governments has given me a unique perspective on the central roles that cooperation and partnership play in NPPD's mission.

An important principle that underlies our work at DHS is that effective homeland security requires close collaboration with the private sector and other stakeholders, and across party lines. I have a long history of working for and with both Republicans and Democrats and I am committed to forging meaningful partnerships that transcend political affiliation. In addition, having served as an attorney in the private sector representing many owners and operators of the Nation's critical infrastructure, including as Security Counsel for the Business Roundtable, I am attuned to the concerns of many of our private sector partners. At DHS, I have increased our engagement with the private sector and other stakeholders and will continue to ensure that transparency and collaboration are guiding principles for NPPD.

Since I joined DHS as NPPD Deputy Under Secretary in 2011, I have focused on improving management processes and enhancing efficiencies by better integrating our cybersecurity, physical infrastructure protection, including federal facilities, and biometric activities. NPPD has improved its operational and management processes through various ongoing efforts, including co-location of its field forces, streamlining cross-component consequence analysis, and combining our operations centers. In addition, though much work remains, we have made progress over the past two years remedying program shortcomings within the Chemical Facility Anti-Terrorism Standards (CFATS) program. These efforts are critically important to the health of the organization and I hope to continue that work in partnership with the Congress.

I am honored to have been nominated by the President for this important position. The security of our Nation is paramount, and DHS and NPPD play critical roles in protecting and preserving the American way of life. If confirmed by the Senate, I pledge to carry out the role of Under Secretary with the Nation's best interest always in mind, with transparency and in close coordination with the Congress.

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?

Response: If confirmed, I commit to be bound by the Oath of Office I will swear to uphold. I have not made any other commitments with respect to the policies and principles I will attempt to implement if confirmed as Under Secretary.

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.

Response: If confirmed as Under Secretary, I will follow all applicable recusal laws and policies.

In connection with the nomination process, I have consulted with the Office of Government Ethics and DHS'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 entered into with the Department's Designated Agency Ethics Official.

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.

Response: No.

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

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

Response: My commitment to the mission of NPPD, to lead the national effort to proteet the Nation's critical physieal and cyber infrastructure, is why I wish to serve as Under Secretary for NPPD. Effective homeland security increasingly requires close collaboration between the private sector and government. NPPD is tasked with working with its partners in and out of government to help secure and keep resilient the functions, goods, and services upon which Americans depend in their daily lives and the nation depends for economic and homeland security. I look forward to continuing to advance NPPD's mission and fostering robust private-public partnerships to keep our Nation's critical infrastructure secure and resilient.

8. For the past few months, you have served as the Acting Under Secretary of NPPD. You have also served as Deputy Under Secretary of NPPD. What are some of the most important things you learned from this experience that you intend to apply as Under Secretary of NPPD?

Response: Though I have learned quite a bit serving with the hardworking men and women at NPPD, several important lessons standout. First, NPPD must continue to strengthen its relationships with its government and private sector partners. The increasing interdependency between physical and cyber infrastructure and across various sectors, requires true partnerships based on trust, mutual understanding of roles and responsibilities stemming from comparative

advantages, and transparency. I hope to continue building those relationships if I am confirmed. Second, privacy and transparency are fundamental pillars that underlie NPPD's mission. DHS and NPPD both have Chief Privacy Officers that oversee programs and operations to ensure that everything we do takes into account the privacy and civil liberties of all Americans. In addition, we publish detailed privacy impact assessments about our programs on the Department's website. I pledge to continue this important work and strive towards the goals of protecting privacy and increasing transparency if I am confirmed. Finally, effective management dictates that we increase the efficiency of our operations and leverage our unique capabilities across physical and cyber infrastructure. As Deputy Under Secretary of NPPD, I oversaw the implementation of numerous management and program reforms in areas ranging from the CFATS program to the co-location of our field forces. In addition, the work NPPD is doing to implement continuous diagnostics and mitigation (CDM) technology across the government and provide a joint assessment capability to our partners will help save money and increase efficiencies.

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

Response: Though events can often dictate priorities, there are important initiatives at NPPD that I am eager to advance if confirmed. The CFATS program has steadily improved since I joined the Department as Deputy Under Secretary. While we implemented a series of programmatic and management reforms to improve the program, there is still much to be done. I pledge to continue the reforms we have instituted and work to make CFATS an efficient and effective chemical facilities security program.

The rapidly growing connection between physical and cyber infrastructure requires that we think about infrastructure protection holistically and understand the potential consequences of an attack across multiple critical infrastructure sectors. If confirmed, I plan to continue efforts underway to better integrate the cyber and physical domains and focus our resources on understanding the consequences of an attack and measures to mitigate those consequences.

Building on the good work that NPPD is already doing, I pledge to strengthen relationships with our government partners and the private sector. Our Nation's security depends on strong public-private relationships. One of NPPD's most important missions is to build robust partnerships that will allow us to better serve the American people by increasing the security and resilience of the critical infrastructure upon which they rely.

Finally, none of these mission objectives can be accomplished without a capable and committed workforce. I will continue to make it a priority to empower the dedicated men and women at NPPD with a clear sense of mission and the tools they need to advance our important mission. In addition, we must continue to recruit the best and the brightest to build our capabilities to meet the challenges we face.

III. Policy Questions

Management

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

Response: Effectively managing staff is an important element of successful leadership. Throughout my career, whether at the CIA, on the House and Senate Intelligence Committees, as the Executive Director of two commissions, or as Acting Under Secretary, I have always abided by the belief that an organization's best asset is the talent of its workforce. The role of the leader is to enable and empower that workforce. I believe that successful leadership is built on finding, developing, and maintaining talented and dedicated professionals. To that end, people work best when they are encouraged to grow their talent, respected by their peers, and supported by their superiors, and understand the importance of the mission they are focused on. I have engaged in several efforts to increase the morale of the workforce, including through regular listening sessions with employees from all levels and in all areas of NPPD and through an award-winning telework program that gives our employees more flexibility to craft their own schedules. I am also firmly committed to helping our employees thrive by providing them with advancement and training opportunities. I have had the opportunity to work with many talented and dedicated professionals at NPPD and I hope to continue that work if confirmed by the Senate.

11. Sequestration has forced DHS to apply non-discretionary funding cuts across the organization. How do you plan, as Under Secretary for NPPD, to do all that you can to sustain NPPD operations and ensure the longer-term stability of NPPD while simultaneously planning around declining budgets?

Response: In fiscal year (FY) 2013, NPPD focused the reductions required by sequestration on non-mission critical spending and sought to find efficiencies to the extent possible. In order to ensure that NPPD is strategically maturing, we will continue to evaluate and identify areas across the Directorate where efficiencies could possibly be found. NPPD has sought to leverage existing tools to accomplish new requirements as well as ensure closer coordination between its programs that are aimed at accomplishing similar objectives.

However, the arbitrary cuts required by sequestration in many cases impacted NPPD's operational programs. In FY 2013, NPPD delayed the development of new National Cybersecurity Protection System capabilities to address emerging cybersecurity priorities, reduced the number of Federal devices that will be covered by the CDM program, and reduced the number of trainings on countering improvised explosive devices that will be conducted with state and local partners. I urge Congress to replace these deep cuts with a more balanced approach that will avoid further reductions that affect NPPD's operational programs.

12. If confirmed, how would you work to improve morale at NPPD?

Response: Through our analysis of the Employee Viewpoint Survey (EVS) results and other data, we have begun to implement a series of initiatives designed to address employee concerns

and improve morale. Our employee input to the EVS surveys and feedback during brown bags, calls with our field forces, and other interactive sessions across the Directorate are some of the mechanisms we use to inform our improvements to the workplace. In addition, we have implemented several new efforts to provide our staff with multiple outlets to express their views to senior leaders. Many of these engagements are bidirectional, giving leadership a chance to ask staff to assist NPPD with improving the workplace environment and morale.

Based on feedback from our outreach efforts, we incorporated the leadership principles of accountability, professionalism, respect, integrity, communication, and empowerment into our leader development programs and the employee on-boarding process. We also established an employee rotational assignment program and a mentor program to provide developmental opportunities to employees. Our senior leader performance plans include a mandatory performance objective that addresses improving employee satisfaction as identified through the Office of Personnel Management (OPM) Federal EVS.

To set expectations of the type of culture desired, we continue to improve our employee onboarding process and leader development programs. NPPD provides its leaders multiple training opportunities to enhance employee capabilities through the development of its basic and refresher supervisory courses as well as development of new leadership training for team leaders and team members. I have led the development of a series of performance management sessions where employees (supervisors and non-supervisors) are provided information on the performance management process. My staff provides timely training during key times throughout the year but also provides ad hoc briefings when requested by individual organizations within NPPD.

I believe NPPD employees are the Directorate's most valuable asset. I hold each of my managers accountable to the leadership principles and encourage them to have an open door policy, listen to the feedback that they receive from their employees, and undertake efforts within their own organizations to continually improve organizational health. If confirmed, I look forward to continuing these efforts.

Critical Infrastructure Protection

13. What do you believe are the key challenges facing our country with respect to protecting critical infrastructure?

Response: The Nation's critical infrastructure—which provides the essential services that underpin American society—is varied, complex, and decentralized. It is owned and operated by public and private sector entities under many different organizational structures, resulting in a large number and wide variety of stakeholders. It is also highly connected, with interdependencies between critical infrastructure assets, systems and sectors existing across geographic, functional and economic boundaries. The complexity and interconnectedness of our critical infrastructure is likely to continue increasing. We must ensure our security and resilience measures also become more sophisticated and interconnected to address threats and hazards that stakeholders in various sectors have in common.

Within this construct, the threat and operating environment for our critical infrastructure is constantly changing. We must continue to focus on an all hazards approach that builds security and resilience to acts of terror, natural disasters, and cyber incidents. We must also recognize the inextricable linkage between physical and cyber critical infrastructure. And we must do so while continuing to work closely with our partners in the critical infrastructure community to develop and implement measures that address the challenges they face.

14. Ensuring the security of the nation's most critical infrastructure and key resources is a vital mission of the Department. Earlier this year, President Obama issued Presidential Policy Directive-21 (PPD-21 Critical Infrastructure Security and Resilience), to coordinate federal infrastructure protection responsibilities and Executive Order 13636 on cybersecurity (Improving Critical Infrastructure Cybersecurity).

    a. What are you plans for implementing the activities required by PPD-21 and EO 13636 and what do you see as the most significant challenges in implementing these initiatives?

    Response:

    DHS, and NPPD in particular, were tasked with various responsibilities under Presidential Policy Directive (PPD) 21 and Executive Order (EO) 13636.

    We are executing much of this work through an Integrated Task Force made up of a number of working groups with representation from across the interagency, State, local, territorial and tribal governments, the private sector, non-governmental organizations, think tanks, and academia. As of August 12, 2013, we have completed 10 deliverables, including a report on incentives to encourage the adoption of the National Institute of Standards and Technology (NIST) cybersecurity framework and the identification of critical infrastructure that, if disrupted by a cyber incident, could reasonably be expected to cause catastrophic consequences. We continue to work on implementation of the PPD and EO and are hard at work on several upcoming deliverables.

    However, the effectiveness of these efforts is dependent upon collaboration with a variety of partners; most importantly, the owners and operators of the Nation's critical infrastructure. We are continually working to improve our outreach to this important community, and have undertaken a number of steps to ensure that our stakeholders have meaningful input into our work.

    While implementation of EO 13636 and PPD-21 is a key step towards securing and making more resilient our Nation's critical infrastructure, continued progress will require sustained effort by both public and private partners, and a recognition of the rapidly evolving risk environment. Though the private sector and government often have different calculations of risk, our continued partnership

will enhance our mutual understanding of those calculations and allow us to work more closely and more effectively to protect and preserve the American way of life.

b. How do you plan to engage the various industry stakeholders in reaching the goals of PPD-21 and EO 13636?

Response: To implement the EO and PPD, we have actively sought the collaboration, input, and engagement of our private sector partners. One of the initial deliverables DHS developed is a consultative process with public and private sector partners. Using the consultative process, DHS developed nine separate working groups and has conducted more than 100 working sessions, involving 1,100 attendees, thus far. Representatives from DHS have also conducted more than 100 briefings to nearly 10,000 attendees since February of this year.

Their input has been vital in crafting deliverables that incorporate the best ideas and lessons learned from public and private sector efforts while ensuring that our information sharing incorporates rigorous protections for individual privacy, confidentiality, and civil liberties.

In addition, DHS launched a platform for posting and sharing public comments and feedback. DHS created a Collaboration Community on IdeaScale for critical infrastructure stakeholders and all interested members of the public to participate in dialogue about strengthening the security and resilience of our Nation's critical infrastructure.

Outside of the working groups, we are engaging the cyber and critical infrastructure community in working sessions, meetings, and with virtual collaboration methods, such as Homeland Security Information Network (HSIN), IdeaScale, and webinars. The format and style of engagement varies according to the needs of the community engaged and the purpose for engagement. The venue and mechanism for engagement is also determined by the outcomes sought and the nature of the constituency involved.

DHS will continue to engage our partners, especially the Sector-Specific Agencies, as it establishes a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and completes additional deliverables.

15. What is the process for identification of critical infrastructure and key resources? Do you believe this system to be effective in identifying the most vulnerable, highest risk, and highest priority critical infrastructure?

Response: Critical infrastructure is defined as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. This definition encompasses vast resources located across the nation. Therefore, NPPD identifies the most vulnerable, highest risk, and highest priority critical infrastructure through two processes annually through extensive coordination with critical infrastructure partners. These are critical infrastructure assets or systems that "would, if destroyed or disrupted, cause national or regional catastrophic effects." The method for identifying critical infrastructure is administered under NPPD's National Critical Infrastructure Prioritization Program (NCIPP).

NCIPP maintains a single classified prioritized list of critical infrastructure systems and assets that are critical to the United States' national security, economic security, and public health and safety. The list is updated each year through a collaborative process with critical infrastructure sectors, state officials, and other critical infrastructure community partners:

- Nomination Phase (March to May): Partners nominate infrastructure that meet criteria for inclusion on the list.
- Adjudication Phase (May): All nominated infrastructure are reviewed to determine whether they meet the established NCIPP criteria based on the justification provided.
- Reconsideration Phase (June to July): Adjudication results are provided to nominators for review and discussion. Nominators submit amplifying information, as appropriate.
- Publication Phase (August): Final list is provided to partners.

The list is prioritized based on potential consequences of a disruption to the critical infrastructure. The resulting list serves as an important component of the Urban Areas Security Initiative and State Homeland Security Grant Program's infrastructure indexes. DHS also uses the list to help partners to prioritize infrastructure protection, response, and recovery activities during incidents. The continued engagement of both private and public sector partners in both updating and using the lists demonstrates the effectiveness of the process.

EO 13636 tasked NPPD with identifying the subset of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. NPPD conducted extensive outreach to the private sector and others to solicit input into the identification process. For example, NPPD facilitated 35 engagement sessions with industry and government representatives from each of the 16 critical infrastructure sectors, and many subsectors or modes, to determine criteria for cyber-dependent critical infrastructure. Our partnership with these stakeholders has been invaluable to our efforts.

NPPD will continue working with our public and private sector partners to identify critical infrastructure vulnerable to physical and cyber threats in order to mitigate risk.

16. Do you consider a coronal mass ejection or a large-scale electromagnetic pulse to present a significant threat to the nation? Is the U.S. electric grid vulnerable to either of those events? If so, what do you see as NPPD's role in mitigating that threat and vulnerability?

Response: The potential consequences from severe solar weather—such as a coronal mass ejection or from Electromagnetic pulse (EMP)—range from temporary system disruptions to permanent physical damage and critical service outages. Naturally occurring solar weather can generate an effect similar to one component of EMP. Those sectors that rely heavily on communications technology, information technology (IT), the electric grid, or that use supervisory control and data acquisition systems are particularly vulnerable. The complex interconnectivity among critical infrastructure sectors means that an EMP incident that affects a single sector will most likely affect other sectors.

Since most critical infrastructure—including virtually all the electric power infrastructure—is privately owned and operated, NPPD works with industry in a number of ways to promote appropriate security investments for a variety of threats, including EMP. NPPD has worked to model and assess EMP effects, and to conduct research and propose solutions to understand and mitigate EMP risks. For example, NPPD conducted a study in 2010 on EMP's potential impact on extra-high voltage transformers and recommended options for hardening these systems from EMP attacks.

Using advanced modeling and simulation capabilities, NPPD prepares and shares analyses of critical infrastructure, including their interdependencies, vulnerabilities, consequences, and other complexities. In addition, NPPD coordinates unclassified and classified briefings and workshops for industry and works to analyze their vulnerabilities and demonstrate potential impacts and costs if those vulnerabilities are left unaddressed. In collaboration with DHS Office of Intelligence & Analysis, NPPD holds quarterly meetings with State, local, tribal and territorial government partners and private-sector representatives, focusing on intelligence and security information sharing.

17. What responsibilities does NPPD have to inform and work with the private sector about threats to critical infrastructure and the people operating those systems?

Response: As coordinator of the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure, DHS has a responsibility to ensure that the right information gets to the right organization in order to support the private sector and other partners. At the core of NPPD's mission is the development and operation of robust public-private partnerships, with an emphasis on information sharing. These partnerships function as effective channels for information sharing and cover both private sector owners and operators and state, local, tribal, and territorial entities. The partnership framework, originally established through the National Infrastructure Protection Plan, facilitates a two-way flow of information.

NPPD works closely with its partners to provide timely, actionable information on imminent or severe threats, leveraging the same organizations and largely the same processes we utilize during our day to day activities. Likewise, we encourage our partners to help us understand the

potential impacts of threats, possible avenues for mitigating these threats, and any unmet requirements which may exist.

18. What steps would you take to ensure that critical infrastructure owners and operators are kept informed of potential threats and in emergency situations?

Response:

Essential to addressing the threat environment is the ability to quickly share threat and mitigation information so that organizations can rapidly understand, adapt to and address changing conditions. Through the partnership framework, NPPD has developed extensive information-sharing mechanisms to facilitate information sharing with critical infrastructure owners and operators during steady state and ongoing incidents. Although each sector shares information differently, there are many avenues to ensure owners and operators across sectors are informed about potential threats and emergency situations.

NPPD has two co-located operational units to share information on physical and cyber threats which serve as the main points for information flow. Both the National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) provide 24/7 support to critical infrastructure stakeholders, both owners and operators, and government partners at the Federal, state, and local levels. Critical infrastructure sectors use HSIN – Critical Information as the main means of sharing information to a trusted and vetted community of owners and operators and other relevant stakeholders. In emergency situations, alerts and warnings of high priority are sent to a list of Federal, state, and local government agencies as well as other private and public stakeholders via email and rapid notification with its Emergency Notification Service. NPPD has also established an Engagement Working Group forum for events requiring heightened information-sharing based on potential threats. The threat-specific Engagement Working Group attendance list includes Federal officials, private sector participants and others as appropriate. Finally, DHS offers the private sector access to security clearances to assist owners and operators of critical infrastrueture in accessing classified information that is relevant to the security and resilience of their assets and systems.

Along with maintaining and strengthening our partnerships, building in mechanisms to disseminate information quickly and to the correct people is essential for making the nation's critical infrastructure more secure and resilient. NPPD is committed to increasing the volume, timeliness, and quality of threat information shared among U.S. public and private sector entities enabling all to better protect and defend themselves against all-hazards, including both physical and cyber threats.

Cybersecurity

19. To what extent are unclassified, civilian federal government networks currently protected against an attack by a determined and sophisticated adversary?

Response: DHS is the lead for securing and defending Federal civilian unclassified IT systems and networks against cyber intrusions or disruptions. Although departments and agencies retain primary responsibility for securing and defending their own networks and critical information infrastructure, DHS assists Federal Executive Departments and Agencies by performing data and report analysis to reduce cyber threats and vulnerabilities, disseminating cyber alert and warning information to promote protection against cyber threats, coordinating with partners and customers to attain shared cyber situational awareness, and providing response and recovery support. Though sophisticated and determined actors pose a challenging threat, the Department is committed to reducing risk and enhancing the security and resilience of our Federal civilian networks through our myriad operations and programs.

20. What challenges does NPPD face in executing its responsibilities in cybersecurity including working with critical infrastructure and civilian federal government networks to prepare for, mitigate, and respond to cyber threats? What is the area where NPPD has provided the greatest value in strengthening federal and/or national cyber security? Are there areas that you think need to be improved or strengthened?

Response: Constantly evolving and sophisticated cyber threats pose unique challenges to the cybersecurity of the Nation's critical infrastructure and its civilian government systems. DHS, as the lead for coordination of the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure, grapples with these challenges every day. For example, DHS is responsible for a large breadth of cybersecurity activities, yet lacks explicit statutory authority to perform these duties. This hinders the Department's ability to fulfill its mission, including to collaborating and assisting certain private sector and government partners. In addition, as we work to develop a national cadre of cybersecurity professionals, we need legislation that provides us with flexible hiring authorities so that we can continue to build a first-rate cyber workforce. The Department has also requested legislation to clarify its authority to deploy EINSTEIN across Federal civilian networks and to provide operational assistance to OMB's oversight of Federal IT network security efforts under Federal Information Security Management Act (FISMA), among other things.

However, despite this statutory ambiguity, NPPD's information sharing and cyber partnership efforts have helped strengthen Federal and national cybersecurity. In 2011, DHS launched the Cyber Information Sharing and Collaboration Program (CISCP), which is designed to elevate the cyber awareness of all critical infrastructure sectors through close and timely cyber threat information sharing and direct analytical exchange. Since December 2011, CISCP has released over 1,100 products containing over 21,000 cyber threat indicators, which are based on information the Department has gleaned from participant submissions, open source research, and from sensitive government information.

In addition, we have worked closely with the private sector during denial-of-service attacks against the financial sector to provide response and mitigation assistance. In conjunction with our law enforcement and intelligence partners, we provided classified cyber threat briefings and technical assistance to help financial institutions improve their defensive capabilities. These developments reinforce the need for greater information sharing and collaboration among

government, industry, and individuals to reduce the ability for malicious actors to establish and maintain capabilities to carry out such efforts.

21. What authorities do you believe the Department needs to effectively and efficiently carry out its cybersecurity mission?

Response: DHS leads the national effort to secure Federal civilian networks and coordinates the overall national effort to protect critical infrastructure and enhance cybersecurity. The DHS cybersecurity mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aid to national recovery efforts for critical infrastructure information systems. In the past four and a half years, cybersecurity has emerged as a top priority for the Department while keeping a steady focus on safeguarding the public's civil rights and civil liberties. The Department executes this mission under an existing patchwork of statutory authorities, presidential directives and Executive Orders spanning multiple Administrations.

While the Nation's dependence on cyber infrastructure has grown exponentially since the Department's founding, the Department's statutory authorities have not kept pace with evolving technologies and reliance on cyberspace by Federal agencies and critical infrastructure. To enable DHS and other agencies to more effectively and efficiently carry out their existing responsibilities, legislative action is necessary. We ask that such legislation:

- Modernize FISMA and reflect the existing DHS role in agencies' Federal network information security policies;
- Clarify existing operational responsibilities for DHS in cybersecurity; and
- Update the Homeland Security Act to reflect organizational maturation of DHS cybersecurity mission and provide acquisition and workforce flexibility to support that mission commensurate with flexibility of federal partners such as the Department of Defense (DOD).

22. The threat to our nation's critical infrastructure from cyber attacks continues to grow. We see clear public examples of this in the ongoing denial-of-service attacks on our financial institutions and the broad intrusion campaigns into our oil and natural gas companies as reported by the Industrial Control Systems Cyber Emergency Response Team. NPPD includes the Office of Cybersecurity and Communications (CS&C), which has broad responsibilities for protecting our communications and cyber infrastructure.

    a. In your view, is the Department doing enough to respond to the rising threat to our critical infrastructure and to the networks of our federal agencies?

    Response: Cyber threats to our critical infrastructure and government networks are diverse in nature and can quickly emerge from a broad range of sources. While these threats are likely to increase in the foreseeable future, NPPD is committed to enhancing the security and resilience of our critical infrastructure and government networks by mitigating the risks posed by these evolving threats. To lead this effort,

NPPD has matured its ability to detect and respond to cyberthreats through the creation of the NCCIC.

The NCCIC provides a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications incident integration for the Federal government, intelligence and law enforcement community, the private sector, and State, local, tribal, and territorial domains. It provides a wide variety of technical assistance to the private sector including vulnerability assessments, incident response, mitigation support and cybersecurity information sharing. Some figures on the NCCIC's efforts in FY'13 include:

- Issuing over 7,500 actionable cybersecurity alerts and products to the Federal government and private sector critical infrastructure partners,
- Providing over 200 alerts, bulletins, and other products to the industrial control systems (ICS) community warning of various threats and vulnerabilities impacting control systems,
- Tracking over 180 unique vulnerabilities affecting ICS products,
- Conducting dozens of assessments across critical infrastructure sectors, and

  Deploying the Cyber Security Evaluation Tool to over 1800 critical infrastructure owners and operators to assist in performing their own cybersecurity self-assessments.

b. How do you see the Department's efforts adapting in the coming years as the threat increases?

Response: While the threat posed by malicious cyber actors continues to evolve, the nature of the Internet ensures that responding to those threats will require the cooperation of a wide variety of partners. DHS must continue to expand our whole-of-nation approach to cybersecurity by leveraging strong partnerships across government, with the private sector, and among our international partners. We must work with all of our partners to actively identify, coordinate, and support responses to incidents that may cause significant harm to critical functions and services. In addition, the rapidly growing connection between physical and cyber infrastructure requires that we understand the potential consequences of an attack across multiple critical infrastructure sectors, and continue to integrate our efforts to ensure the security and resilience of both the cyber and physical infrastructure domains. DHS will continue to take the lead role in coordinating these efforts so that the unique skills of all partners can be put towards mitigating these evolving threats.

Dealing with this increasing threat also requires that we preserve and protect privacy and civil liberties and operate in a transparent manner. DHS and NPPD have built

strong privacy protections into all of its cybersecurity efforts. The Department's Chief Privacy Officer, and NPPD's privacy office, work closely with our operational teams to ensure that privacy, civil liberties, and transparency considerations are baked into each and every program. We also publicly post Privacy Impact Assessments that detail how the privacy protections operated in each program on the Department's public website. Privacy, civil liberties, and transparency underpin our cybersecurity mission at NPPD, and we will continue to uphold them as a cornerstone of our security efforts.

23. As responses to recent cyber incidents have shown, cybersecurity requires an all-of-government approach and shared responsibilities with the private sector. These relationships work best when the roles and responsibilities of involved entities are clearly established and when personal trust has been established between those working on the issues.

    a. The relationships between NPPD, the Federal Bureau of Investigation, and the National Security Agency are particularly important. How will you cultivate the relationships with senior leadership of these two agencies and other?

Response: I could not agree more that successful response to cyber threats requires a whole-of-government approach to identifying, attributing, mitigating and responding to malicious activity. This means leveraging all homeland security, law enforcement, intelligence, and military authorities and capabilities. While DHS, DOD, and the Department of Justice (DOJ) have distinct cybersecurity missions, processes, and partners, we have a shared responsibility to support each other with our unique capabilities to address the key cyber threats facing the Nation. Recent cyber incidents over the past several years have allowed us to work and exercise together to leverage our unique roles and specific responsibilities as part of a broader Federal effort to counter cyber threats. I will continue to engage my counterparts at DOD and DOJ to address the key cybersecurity policy and operational issues by:

- Prioritizing the direct connections between our key operations centers for shared situational awareness of specific malicious cyber activity;
- Enhancing the synchronization of our incident response and analytical activities; and,
- Continuing development of specific operational processes to align private sector notification and engagement.

    b. How will you establish trust and effective collaboration with privately owned critical infrastructure?

Response: Direct real world collaboration is the best way to build trust between government and the private sector. I will continue to ensure that DHS works directly

with our private sector partners to identify the cybersecurity threats that most directly impact their networks by fostering collaboration at the analyst level, where the best sharing of key technical data happens and at the Chief Executive Officer (CEO) level where decisions are made based on enterprise risk management I will also work to provide timely and actionable information to inform those decisions and mitigate risk through programs such as the Cybersecurity and Information Sharing and CISCP and the Enhanced Cybersecurity Service Program (ECS). Finally, I will continue to engage them in strengthening our public private partnership by participating in trusted communities to enhance collaboration and build shared threat knowledge.

c. What do you see as the appropriate role for NPPD in private sector cybersecurity?

Response: As the civilian Department at the intersection of public-private cybersecurity efforts, DHS is a focal point for coordinating cybersecurity efforts with the private sector to help better inform risk management decisions. Enhancing understanding about cyber threats and vulnerabilities helps to reduce these risks and encourages partners to mitigate their consequences. This role requires the Department to expeditiously support private sector partners with cyber intrusion mitigation and incident response by providing onsite analysis, mitigation support, and assessment assistance. Initiating technical assistance with any private company is a sensitive endeavor that requires trust and strict confidentiality. DHS's efforts to focus on computer network defense and protection rather than law enforcement, military, or intelligence functions help foster this trust and also provides valuable tools, such as PCII, for maintaining this confidentiality.

24. What progress has NPPD made in encouraging information sharing within the private sector as it relates to cybersecurity, including but not limited to cybersecurity of industrial control systems like supervisory control and data acquisition systems? What challenges remain? What recommendations would you make to improve multi-way cybersecurity information sharing between researchers, private industry, and the federal government?

Response: DHS has made significant progress in expanding information sharing activities with the private sector. In 2011, DHS launched the Cyber Information Sharing and Collaboration Program (CISCP), which is specifically designed to elevate the cyber awareness of all critical infrastructure sectors through close and timely cyber threat information sharing and direct analytical exchange. Through CISCP, participating private sector entities are able to share data directly with government in a transparent manner that ensures strong privacy protections. Hundreds of products and thousands of indicators have been shared through CISCP already.

Another avenue for information sharing is the newly operational ECS. This effort provides another layer of protection to critical infrastructure entities by allowing Commercial Service Providers to utilize sensitive government cyber threat information for intrusion prevention services.

The Department has also worked to provide the private sector with tools to increase sharing with other private partners through the development of standardized indicator sharing tools such as STIX and TAXI. These tools make a standardized format and protocol for transferring malware indicators in a machine readable format so that partners with different systems can utilize one common language. This effort has already been adopted by the Financial Services Information Sharing and Analysis Center for use with their partner organizations.

While DHS has a strong track record of working closely with private sector companies to provide warnings of cyber vulnerabilities and threats, many companies who would like to share cyber security information with the Department are held back by unclear statutory authorization for such activities and perceived liability concerns. Some companies agree to share information back to DHS because they understand the need to get threat information into the hands of other private sector partners that they rely on. However, some companies believe that they are prohibited from sharing certain cyber threat information with the U.S. Government.

The Administration continues to believe that carefully crafted information sharing provisions that provide clear authority to the private sector to share pertinent information with the Department, and narrowly scoped liability protections, should be a part of a comprehensive suite of cybersecurity legislation. It is vital that such legislation also respect the role of civilian versus national security entities, and enhances transparency along with privacy and civil liberties protections. The Department will continue to work with Congress to achieve these goals and enhance the security and resilience of our critical infrastructure.

25. Currently, many distinct components and offices within DHS play a role in the Department's cybersecurity mission including but not limited to: CS&C, the National Cybersecurity and Communications Integration Center ("NCCIC"), the Office of Policy, and agencies like the Coast Guard and the Transportation Security Administration.

    a. Please describe the scope of the Department's current work in the area of cybersecurity.

    Response: DHS plays a broad role in national cybersecurity efforts. As directed under Presidential Policy Directive 21, the Secretary is responsible for coordinating Federal Government responses to significant cyber incidents affecting critical infrastructure, consistent with statutory authorities. NPPD leads the Department's efforts in infrastructure protection and resilience and securing unclassified Federal civilian networks. Several DHS law enforcement components also play critical roles in the national cyber effort including Immigration and Customs Enforcement (ICE) and U.S. Secret Service (USSS) offices who both investigate and prosecute cyber-crimes. Finally, several components also act as the lead Sector Specific Agencies for sectors that have important roles in national cybersecurity efforts including the Communications, Critical Manufacturing, Emergency Services, Transportation (including roles for the Transportation Security Administration [TSA] and the U.S. Coast Guard [USCG]), and Information Technology sectors.

b. What do you see as its major accomplishments? Identify the components and offices that contributed to these accomplishments.

Response: DHS has had many recent accomplishments in providing cybersecurity response to the Financial Sector, increasing awareness about threats to our Oil and Natural Gas Sector, establishing a CEO-level working group with the electric sector, working with the interagency to stop intellectual property theft, and cracking down on cybercrime.

DHS' NCCIC has worked closely with the private sector and other government partners during the recent series of distributed denial-of-service incidents against the Financial Sector. Together with our interagency partners, we have provided classified cyber threat briefings and technical assistance to help banks improve their defensive capabilities. This includes identifying and releasing hundreds of thousands of related IP addresses and supporting information in order to help financial institutions and their IT security service providers improve their defenses. In addition to sharing information with these private sector entities, DHS, in conjunction with the Department of State (DOS), has provided this threat information to more than 120 international partners, many of whom have contributed to our mitigation efforts. These developments reinforce the need for greater information sharing and collaboration among government, industry, and individuals to reduce the volume and severity of cyber attacks.

NCCIC's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has also been deeply engaged in supporting industry partners during recent cyber intrusions in the Oil and Natural Gas Sector. In March of 2012, DHS identified a campaign of cyber intrusions targeting natural gas pipeline sector companies with spear-phishing e-mails that dated back to December of 2011. Stolen information could have provided an attacker with sensitive knowledge about industrial control systems, including information that could allow for unauthorized operation of the systems. Responding quickly, DHS immediately began an Action Campaign to alert the community of the threat and offered to provide assistance. In May and June, DHS deployed teams for onsite assistance to two of the organizations targeted in this campaign and partnered with DOE and others to conduct briefings across the country, including in the cities of Arlington, Virginia; New York City; Washington, DC; Chicago; Dallas; Denver; San Francisco; Anchorage; Houston; and Atlanta. Over 500 private sector individuals attended the classified briefings and hundreds more for the unclassified briefings, and the Department has released numerous actionable alerts following up on these and other threats to the sector.

In addition to these attacks, we also face a range of traditional crimes now perpetrated through cyber networks. These include child pornography and exploitation, as well as intellectual property theft and financial fraud, all of which pose severe economic and human consequences. For example, in March 2012, the USSS worked with ICE to arrest nearly 20 individuals in its "Operation Open Market," which seeks to combat

transnational organized crime, including the buying and selling of stolen personal and financial information through online forums.

Various cyber actors have also been engaged in the theft of intellectual property, trade secrets, and other sensitive business information. They use a variety of techniques to infiltrate targeted organizations and steal confidential or proprietary data. DHS, in collaboration with the Federal Bureau of Investigation (FBI) and other partners, has released Joint Indicator Bulletins containing cyber threat indicators to help private sector partners take action to stop this activity and protect them from this theft. ICE has also lead coordination of "Operation In Our Sites," that targets distribution of counterfeit and pirated items over the internet. To date this operation has seized a total of 2,075 domain names, made fifteen arrests and seven indictments, with eight convictions.

Finally, in late May 2013, the USSS led the investigation, in close coordination with ICE and the Global Illicit Financial Team, into Liberty Reserve, a transnational online payment processor and money transfer system. It is alleged that Liberty Reserve is used by criminal elements worldwide to launder money and distribute illegal proceeds. USSS arrested five individuals and seized bank accounts containing approximately $20 million located in eight countries. Overall, Liberty Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds. The United States Attorney's Office for the Southern District of New York is prosecuting this case.

c. If confirmed, what would you do to strengthen the NCCIC?

Response: The NCCIC is the central hub of NPPD's cybersecurity mission, and its capabilities have grown significantly over the past year. If confirmed, I fully intend to continue this trend, and will focus on ensuring that NCCIC continues to be staffed by top analysts who work closely with government, private sector, and international partners to identify, analyze, share information about and mitigate malicious cyber activity. If confirmed, I also intend to enhance coordination between the co-located NCCIC and NICC, including the development of an integration function to enhance situational awareness of physical consequences of cyber incidents.

26. Bureaucracy within the Department and between partner agencies can be a major hindrance to accomplishing its cybersecurity mission in a timely fashion. For example, for cyber threat information to be most useful, it must be timely and actionable. However, problems with declassification at other agencies and the processing of clearances often slows the sharing of such information.

    a. How do you plan to formalize such processes within NPPD to make them more efficient and repeatable?

Response: NPPD maintains existing processes for immediately requesting tearlines of classified information and when appropriate, declassification of actionable cybersecurity information from the classifying agency. NPPD will also continue to communicate clearly and effectively with our critical infrastructure partners regarding the appropriate form of agreement and governance that enables them to be cleared to receive relevant classified data defined by government mission needs and the threat environment.

b. How do you plan to work with other agencies on these issues?

Response: Recent operational efforts have driven the interagency to begin to streamline this process and I will continue to engage our Federal partners, including the intelligence community, defense, and law enforcement partners to emphasize the importance of expeditiously providing tearlines and declassified materials.

27. Maintaining a qualified workforce for cybersecurity is a challenge faced in government and in the private sector given that there are relatively few skilled experts compared to the number of positions that need filled. Federal agencies, however, may face the greater challenge of competing for these individuals with the private sector, which can often pay more and hire more quickly.

a. How do you plan on developing and maintaining a world-class cyber workforce within NPPD?

Response: NPPD has engaged multiple internal initiatives and Departmental initiatives to continue building a world-class cyber workforce. Through close work with the DHS Management Directorate's Office of the Chief Human Capital Officer, we have begun to address recommendations made by the Secretary's Homeland Security Advisory Council Task Force on Cyber Skills. As part of this work, the Department has identified 1200 positions performing mission critical cybersecurity work, and experts from across Components are developing and executing Department-wide human capital strategies, policies, and programs intended to enhance that workforce.

Currently, the Department is finalizing training and evaluation standards aimed at ensuring cybersecurity employees have access to the highest quality training and that new DHS hires are recruited and developed in alignment with Departmental standards. In addition, several pilot programs have been launched to grow the pipeline for DHS cybersecurity talent through targeted outreach to academic institutions as well as organizations dedicated to veterans' employment.

DHS, through NPPD, jointly sponsors the National Centers of Academic Excellence (CAE) programs with the National Security Agency. DHS has contributed significantly to the recent development of new criteria and focus areas for CAE-designated institutions, allowing DHS to enhance its recruitment efforts from among

the CAE community.

In addition, DHS co-sponsors the CyberCorps(R): Scholarship for Service (SFS) program with the National Science Foundation. SFS recipient students receive scholarships in the last two years of their college or graduate degree program and in return serve the equivalent number of years in a government cybersecurity role. Each year, NPPD is one of the most active recruiters of top-notch cybersecurity talent for interns and full-time hires at the annual SFS job fair in January and continues to hire SFS recipients throughout the year.

NPPD is also increasing its outreach to the K-12 population to promote cybersecurity careers and studies. One way it does so is through the Integrated Cybersecurity Education Communities project, which holds cyber education summer camps for high school teachers and students, with a goal of affecting 1.7 million students in cyber education over ten years.

Finally, we continue to engage OPM to provide the necessary skill codes in order to bring on cyber personnel in a streamlined manner, with pay and benefits reflective of their technical designation.

Though these efforts have helped NPPD build its first-rate cyber workforce, we need legislation that provides flexible hiring authorities, so that we can keep up with our Federal partners. These authorities can help us build and maintain the necessary talent to meet the challenges facing the Nation's critical infrastructure.

b. Do you believe DHS needs additional hiring authorities for cybersecurity workers so it can better compete with other federal agencies and with the private sector?

Response: Attracting highly-qualified technical experts to enter government service over the private sector can be difficult, and the variation in hiring and pay authorities across the federal government frequently makes it challenging for DHS to recruit cyber talent interested in federal service.

We continue to recommend that the Secretary of Homeland Security be provided with hiring and pay authorities commensurate with those of the DOD. Specifically, legislation is needed to give the Secretary authority to establish positions in the excepted service, such that the Secretary could make direct appointments, set compensation rates, and pay additional benefits and incentives. The Secretary would also be authorized to establish a scholarship program for employees to pursue an associate, baccalaureate, advanced degree, or a certification in an information assurance discipline.

These additional authorities would allow NPPD and other DHS Components to compete better with the private sector and the military and intelligence agencies in terms of both salary and hiring time.

c. What are your thoughts on the need to create a more clearly-defined cyber career path at DHS from entry-level positions to senior leadership?

d. **Response:** I am committed to strengthening the career path for cybersecurity professionals at NPPD. The Department is working to develop the training, credentialing and evaluation standards necessary to create a more clearly-defined career path. We are also seeking a special technical designation in order to accommodate hiring technical performers at appropriate levels of management responsibility and grade, to create a happier workforce with a clear path for development. DHS' cyber workforce consists of a wide variety of critical cybersecurity skill sets that can be woven into a unique DHS career path that encourages retention of talent and grooms future cyber leaders from within the Department.

How will you maintain strong morale and loyalty among the workforce?

Response: I am committed to strengthening and maintaining a robust, satisfied, and motivated workforce.

At NPPD, we have implemented several new efforts to provide our staff with multiple outlets to express their views to senior leaders. Many of these engagements are bi-directional, giving leadership a chance to ask staff to assist NPPD with improving the workplace environment and morale.

Based on feedback from our outreach efforts, we incorporated the leadership principles of accountability, professionalism, respect, integrity, communication and empowerment into senior leader performance plans and the employee on-boarding process. We also established an employee rotational assignment program and a mentor program to provide developmental opportunities to employees.

NPPD is privileged to have a dedicated and talented workforce that comes to work each day wanting to make a difference. We have worked to provide them with a clear sense of mission and accomplishment. Though we have much more to do, this will continue to be a priority at NPPD and within the Department.

e. How will you ensure that senior leadership have good reason to stay for several years, that vacant positions are filled expeditiously, and that policy and direction remain steady between successive officials?

Response:

Cybersecurity is a dynamic environment requiring a specialized skillset that bridges technical and policy expertise. The Department is committed to growing and retaining its cyber workforce, and is putting the conditions for success in place by addressing the recommendations of the Secretary's Homeland Security Advisory Council Task Force on Cyber Skills. Hiring and pay authorities commensurate with

those of the DOD, as mentioned above, would enable NPPD and other DHS Components to better compete with the private sector and the military and intelligence agencies in terms of both salary and hiring time.

NPPD's most senior leadership has provided important continuity and I am committed to continuing to provide steady leadership in a very dynamic environment.

f. Why do you believe NPPD has seen such high turnover in key cybersecurity leadership positions over the past few years?

Response: I believe employees are our most valuable asset, and have strived to ensure our leaders are given the tools and support they need to perform their mission effectively. Although there has been some turnover in top-level cybersecurity positions, the core Senior Executive Service employees of the Office of Cybersecurity & Communications have remained stable, and have performed admirably in a dynamic environment. I will continue to work hard to ensure we fit the right personnel in leadership roles and provide the empowerment necessary to accomplish the mission.

Chemical Site Security

28. In November 2011 an internal DHS management memo was leaked to the press, detailing ongoing management and programmatic issues in the CFATS program.

a. Since the leaking of the November 2011 internal DHS management memorandum regarding the CFATS program, what plans have been put in place and steps taken to address the problems laid out in the memorandum?

Response: During my tenure as Deputy Under Secretary, I oversaw implementation of a comprehensive Action Plan to address management and program concerns. Specifically, the Action Plan is comprised of 95 action items to address program and management issues raised in the memo. As of September 1, 2013, 91 of the 95 action items contained in the current Action Plan have been completed. The Infrastructure Security Compliance Division (ISCD) is on track to complete the four remaining action items in FY 2014.

b. What initiatives have been undertaken to improve the workforce issues laid out in the memorandum?

Response: NPPD has undertaken significant efforts to address workforce issues within ISCD. As part of the Action Plan implementation, ISCD realigned its organizational structure to meet operational and management objectives going forward, including with regard to supervisor-to-employee ratios both at headquarters and in the field. This includes a realignment of the field operations in order to meet the heightened pace of compliance assistance visits and authorization inspections, and the expected commencement of compliance inspections.

ISCD also updated and revised its internal inspections policy and guidance materials for conducting inspections. After releasing the updated guidance materials, ISCD conducted five inspector training sessions, which focused on the updated policy, procedures and related materials to better prepare Chemical Security Inspectors to resume authorization inspections. ISCD has improved its inspection process over the past year and a half, and continues to identify efficiencies to keep moving forward.

NPPD is continuing to use a balanced approach in its hiring practices that allows for internal career growth within the organization as well as external recruitment practices, to bring in qualified personnel and improve the organizational culture. NPPD has hired permanent leadership for ISCD, including the director and deputy director, who are committed to making the program a success. In addition to filling senior leadership positions, we are working to ensure that all employees are in positions in which they can perform most effectively and that are best suited to their skills and expertise. ISCD has made improvements to internal policies on topics such as telework, and has worked to provide employees with concrete performance plans that contain clearly defined and actionable measures.

c. What is your current assessment of the CFATS program and what are the remaining greatest systemic problems and challenges for the CFATS program and your plans for addressing these problems and challenges?

Response: Over the past 18 months, the Department has made significant progress in advancing the CFATS program. This progress includes implementation of a revised SSP review process that has increased the pace of SSP reviews; additional training for inspectors on updated inspection protocols, which has allowed for an increased Authorization Inspection pace; and the documentation of a number of critical processes through Standard Operating Procedures. As of September 1, 2013, these efforts have enabled ISCD, the division responsible for implementing CFATS, to authorize more than 600 SSPs, conduct more than 400 Authorization Inspections, and approve more than 240 security plans. ISCD is now on pace to authorize, inspect, and approve between 30 and 50 security plans per month and is continuing to explore ways to further increase the pace of performance as we move into Tier 3 and Tier 4 plan reviews.

The Department believes that the CFATS program is strong and continues to make the nation more secure; however, we recognize that there is more work to do. NPPD continues to work on methods to reduce the time it takes for a facility-submitted site Security Plan (SSP) to be reviewed and approved. ISCD will continue to work with industry stakeholders on alternate security program models that have the potential to make the CFATS program more efficient and effective. ISCD also is exploring ways to streamline the SSP inspection process to reduce the time and resources required to conduct inspections.

In addition, as a part of our commitment to continue moving the CFATS program forward, NPPD is conducting a thorough review of the tiering process. In support of this, NPPD has implemented a phased approach, which is captured in the ISCD Action Plan and includes: documenting all processes and procedures relating to the tiering methodology; conducting an internal NPPD review of the tiering process; and initiating an external peer review of the risk assessment methodology. We expect the peer review to provide input on how DHS can enhance the CFATS tiering models as appropriate. After receiving the report from the peer review, DHS will determine next steps to address any issues.

d. What steps have been completed and which remain incomplete in the action plan developed in response to the internal DHS management memorandum? If confirmed as Under Secretary, how would you plan to address to act on the uncompleted items?

Response: Currently, 91 of the 95 action items contained in the Action Plan, developed in response to the internal DHS management memorandum, have been completed. The completion of these 91 Action Plan items has directly resulted in improvements and progress made by ISCD over the last year and a half. For example, the division realignment ensured staff were placed in appropriate positions and were available to carry out necessary work within the division, like SSP approvals. ISCD provided supervisory training to all ISCD supervisors to ensure supervisors had the skill set to manage staff and ensure programmatic changes were implemented. The formalization and documentation of a number of standard operating procedures, and the updating and implementation of new basic inspector training, ensured SSPs were reviewed, authorized, and inspected according to consistent guidelines. Finally, the Action Plan provided a pathway for ISCD to reinitiate authorization inspections.

The four action items that remain open focus on the refinement of the Chemical Security Assessment Tool to make it more efficient and effective, the refinement of the internal information technology system that supports the scheduling and management of inspector activities, additional analysis on the optimum staffing level for the Division, and the development of a human capital strategic plan. Significant progress has been made on all four of these initiatives, and all are on track to be completed in FY 2014.

e. Do you believe the program has contributed to improving security at chemical facilities?

Response: Yes, the Department believes that implementation of the CFATS program has improved security at chemical facilities. The non-prescriptive nature of the CFATS program has resulted in chemical facilities implementing cost-effective approaches to improve security that take into account the unique characteristics and risks associated with their facilities. Additionally, CFATS has helped reduce the

overall risk to the nation from chemical facilities, as more than 3,100 facilities have elected to modify their chemical holdings, or make other changes, that have resulted in the Department determining that those facilities no longer present a high security risk.

29. The West Fertilizer Company explosion earlier this year exposed several shortcomings with oversight of chemical plants. As one example, the West Fertilizer Company had failed to file a top screen in accordance with the program requirements. Until the time of the explosion, little had been done to find these non-compliant facilities and take action against them. In a letter sent to Chairman Carper on August 1st, DHS noted that a "reinvigorated effort" had begun to cross-reference DHS and EPA facility data to identify these "outliers" and that the initial matching had been completed in June 2013.

a. How do you intend to strengthen information sharing between DHS, EPA, and other government agencies to improve implementation of the CFATS program?

Response: Since the establishment of the CFATS program in April 2007, NPPD has conducted significant outreach to the regulated community and other interested or affected entities so that they are aware of the program's requirements. NPPD and ISCD management and staff have presented at hundreds of security and chemical industry gatherings and participated in a variety of other meetings. NPPD's chemical inspectors actively work with facilities, local stakeholders, and governmental agencies across the country. Collectively, they have participated in more than 5,260 meetings with Federal, state, and local officials; held more than 4,680 introductory meetings with owners and operators of CFATS-regulated or potentially regulated facilities. As part of this outreach initiative, NPPD and ISCD leadership have regularly updated affected sectors through their Sector Coordinating Councils and the Government Coordinating Councils—including the Chemical, Oil and Natural Gas, and Food and Agriculture Sectors. To promote information sharing, ISCD has developed several communication tools for stakeholder use, including: the Chemical Security website *(www.DHS.gov/chemicalsecurity)*; a help desk for CFATS-related questions; a CFATS tip-line for anonymous chemical security reporting; and CFATS-Share, a web-based information-sharing portal that provides certain Federal, state, and local agencies access to key details on CFATS facility information as needed.

NPPD anticipates information sharing efforts will be strengthened as a result of the initiatives in EO 13650 Improving Chemical Facility Safety and Security. As one of the tri-chairs of the Working Group, and the Secretariat for the overall EO, NPPD is actively participating in all sections of the EO. In particular, NPPD is leading the sub-working group for Section 5 that requires the agencies to put forth three deliverables that enhance information collection by sharing across agencies to support more information decision making, streamline reporting requirements, and reduce duplicative efforts.

Prior to the issuance of the EO, NPPD had begun the process of systematically cross-walking other Federal agency data with the CFATS data. NPPD coordinated with EPA to review submissions made to EPA's Risk Management Plan (RMP) program to identify facilities that likely possessed a threshold amount of a CFATS chemical of interest but appear not to have submitted a Top-Screen to DHS.

Additionally, DHS has shared facility data with the State of Texas and is working collaboratively with the Bureau of Alcohol, Tobacco, Firearms and Explosives to conduct a similar data cross walk with involving data regarding federal explosives licensees and permittees. Efforts to ingest this data began as the analysis on the EPA RMP data was completed. DHS anticipates replicating the cross-walk process with data from OSHA as well.

NPPD anticipates integrating the lessons learned from the individual cross-walks into the deliverables for the EO in order to improve information sharing and to make data sharing a routine process.

b. Do you believe that the CFATS program should take a more aggressive approach to non-compliant facilities and if so how should it be done?

Response: The CFATS-regulated community is expansive and dynamic and DHS is committed to pursuing all reasonable measures to identify potentially noncompliant facilities and urge them toward compliance. In order to further reduce the likelihood that potential high-risk chemical facilities intentionally or unintentionally avoid identification under the CFATS program, the Department is engaging in a variety of efforts to increase our efforts at identifying non-compliant facilities.

One of those efforts, as described above, is actively participating in the EO 13650 initiatives in five key areas:

1. Improving operational coordination with State and local partners;
2. Enhancing Federal coordination;
3. Enhancing information collection and sharing;
4. Modernizing policies, regulations, and standards; and
5. Identifying best practices

This work will result in increased coordination, information sharing, and collaboration between Federal, state, local, tribal, and territorial entities and enable NPPD to review data to determine facilities possibly not in compliance with the CFATS reporting requirements.

Chemical facility security is a shared responsibility with the private sector and government stakeholders. DHS is committed to working with industry stakeholders, both in the field with regulated facilities and state and local government officials, as well as on a national level with chemical industry associations. Therefore, ISCD is expanding outreach efforts to raise awareness of CFATS requirements with stakeholders. ISCD has expanded outreach efforts to include identification and prioritization of stakeholder communities by segment; identification and engagement of agencies and organizations to assist with outreach; identification of broad educational avenues and opportunities; and identification and analysis of outreach opportunities through the chemical industry supply chain.

As an example of the outreach, NPPD coordinated with the Texas State Fire Marshall and Texas State Chemist to secure a list of Texas facilities that are involved with that sale and distribution of ammonium nitrate in the state. Similar to the cross-walk with the EPA RMP data, DHS sent letters to possible non-exempt facilities in Texas instructing them to file a Top-Screen or provide an explanation as to why it does not need to submit a Top-Screen. The Department continues to operate its CFATS Tip Line and follow up on any reports of potentially non-compliant facilities submitted through the Tip Line.

Finally, the Department is prepared to use its statutory authority to issue an Administrative Order if a facility is found to be non-compliant with any aspect of the CFATS program, including the submission of a Top-Screen. If DHS determines a facility should have submitted a Top-Screen and did not, the Department may issue an Administrative Order which identifies the specific steps the facility must take to come into compliance and provide the facility with a reasonable opportunity to correct its non-compliance. If the facility continues to be in non-compliance, the Department may issue a civil penalty and/or direct a facility to cease operations for violating the previously issued Administrative Order.

30. As you stated in testimony before the House Appropriations Subcommittee in September 2012, "Many members of the regulated community and their representative industry associations have expressed interest in exploring ways to use the Alternative Security Plan (ASP) provisions of the CFATS regulation to streamline the security plan submission and review process." We understand that DHS, along with the American Chemistry Council, worked to devise an Alternative Security Plan template for industry.

    a. In your view how successful has the ASP template been, in terms of both industry compliance and DHS's review and approval time?

Response: The Alternative Security Programs (ASPs) present value both to DHS and industry in helping to streamline the development and review of security plans. ISCD has worked, and continues to seek opportunities to work, collaboratively with industry to identify subsectors that may benefit from the development of a new ASP template. One ASP template was published for use by the American Chemistry

Council, in late 2012. Many other members of the regulated community and their representative industry associations have expressed interest in exploring ways to use the ASP provisions of the CFATS regulation to streamline the security plan submission and review process. ISCD shares this goal and has been holding discussions with industry stakeholders about their development of ASP templates on behalf of their members, including the National Association of Chemical Distributors, Agricultural Retailers Association, and the Electric Sector ASP Cooperative. We expect that as more associations work to develop ASP templates, and those facilities who use the templates receive authorization and approval of their ASPs, we may see an increase in the total number of ASPs submitted.

b. What lessons can be learned from the ASP process and how can they be applied to other continuingly problematic parts of CFATS?

Response: One primary lesson learned to date on ASPs is that the instructions relating to both ASPs and SSPs must include a clear articulation of the level of detail that is necessary to be included in an ASP or SSP for the Department to determine whether the ASP or SSP meets all applicable risk-based performance standards (RBPS). A second lesson learned is ASP templates allow facilities to document their individual security strategies for addressing their security risks and meeting applicable RBPS under CFATS in a clear and concise manner and that accounts for individual business operations. The existing ASP does this by allowing corporations to cover the fundamentals of their security, such as restricting the area perimeter, securing critical assets, screening and controlling access, cybersecurity, training, and response within their own specific corporate models.

Finally, the Department's engagement with industry to develop ASP templates is a prime example of how the CFATS program can work with industry to develop the tools that answer regulatory requirements while also accounting for industry realities. ISCD will continue engaging with industry on ASPs and other aspects of program implementation.

Federal Protective Service

31. How will you ensure accountability of contract guards at federal facilities working for the Federal Protective Service (FPS)?

Response: The Federal Protective Service (FPS) provides contract oversight in accordance with Federal acquisition regulations and DHS policies. The security companies doing business with FPS are responsible for ensuring that their employees/guards meet contractual requirements. NPPD is ensuring that FPS officials responsible for the oversight of these contracts are fully trained to carry out their oversight responsibilities. In order to augment its existing contract oversight personnel, FPS is in the process of hiring full-time Contracting Officer Representatives (COR) nation-wide. Further, FPS is developing an interim tool for use by CORs to assist in

tracking guard-related training and certification information and to assist in the monitoring of these contracts.

Using Federal regulations and DHS policies, our Contracting Officials (like other DHS Contracting Officials) hold contract companies accountable for performance, and FPS consistently exceeds DHS published goals for conducting timely assessments via the Contractor Performance Assessment Reporting System (CPARS). CPARS is the official system of record used by DHS for documenting contractor performance information.

32. Does FPS currently have a comprehensive system for contract guard oversight? Does that system allow the Department to independently verify contract guard training and certification and that contract guards are at their assigned post as they report? If not, when will such a system be in place?

Response: FPS does have a comprehensive method for providing security company contract oversight and is looking into new or improved technology that could assist FPS in performing its oversight responsibilities more efficiently. FPS uses a variety of methods for gathering information/data to support its efforts of providing and documenting contract oversight.

These methods include the collection and review of information submitted directly from contract companies, including certification documentation, quality control reports, review of sign in/out documentation prepared by guards, information provided by FPS Inspectors during the conduct of post inspections, information gathered during administrative audits of guard files, and direct government oversight of guard performance. These methods are largely manual in nature.

Through its collaboration with the DHS Science and Technology Directorate (S&T), FPS is reviewing alternative tools to improve contract oversight, to include validation of post coverage and guard certification information.

33. During your time as Deputy Under Secretary at NPPD, what did the Federal Protective Service do to prevent duplication of facility security assessments (FSAs)? What changes will you implement as Under Secretary to prevent duplication of FSAs?

Response: While FPS does not have the authority to prevent other agencies from conducting their own assessments, they do keep tenants informed about FPS's facility security assessment process and requirements. If and when FPS learns that a tenant is conducting an independent security assessment, FPS reaches out to remind the tenant that there is no requirement for a separate assessment. Going forward, FPS will continue to conduct outreach about FPS's requirements and processes, and their value, in order minimize duplicative efforts with other agencies.

34. What is the status of development of the Modified Infrastructure Survey Tool (MIST)? How will you ensure that development and deployment of MIST will stay on time and on budget?

Response: The Modified Infrastructure Survey Tool (MIST) development effort was completed on schedule, with Argonne National Laboratory delivering the system to the Government on March 30, 2012. MIST is currently deployed for use in the field; 1,660 facility security assessments (FSAs) have been completed to date. FPS has FSA program managers that oversee operational use of the tool.

US- VISIT

35. 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. In FY2013, the Obama Administration proposed moving US-VISIT out of NPPD and placing its core functions within Customs and Border Protection, arguing that it is essentially a border security program. The Appropriators, however, kept most of US-VISIT in NPPD.

    a. Where do you believe that US-VISIT should be located within the Department?

Response: The Consolidated and Further Continuing Appropriations Act, 2013 (Public Law 113-6) transferred the core of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program staff to establish the Office of Biometric Identity Management (OBIM) under NPPD. The Act also transferred the program's overstay analysis mission to ICE as well as the entry/exit policy and operations mission to CBP. This realignment allows OBIM to focus directly on biometric identity capabilities. OBIM fulfills one of NPPD's strategic goals by delivering enterprise Identity Services that enable Homeland Security Missions. By matching, storing, sharing, and analyzing biometric data, OBIM provides decision makers with rapid, accurate, person-centric, secure identification and analysis services to make more informed decisions. OBIM helps to protect our critical infrastructure, facilitate legitimate travel and trade, and help to secure our borders.

    b. Do you believe the US-VISIT program is an identity management program, a border security program, or a terrorism prevention program?

Response: OBIM is an enterprise-level biometric identity services provider and is essential in supporting a wide array of DHS missions. Immigration officers, law enforcement agents, DHS mission partners, other Federal Departments, the Intelligence Community, and foreign partners all depend on OBIM's biometric identity services daily to make decisions. Biometric identity services assist front-line decision makers whether the people they encounter should receive or be denied certain benefits or access rights; whether an individual poses a threat to the United States; or has violated the law.

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?

Response: OBIM will focus its efforts on providing identity services to its Federal, state, local, and international partners. OBIM is improving biometric data sharing with (1) the DOJ, and DOD towards a "whole of government" approach to identity services; (2) the Intelligence Community; and (3) trusted international partners, in support of national security and public safety. DHS customers currently include: U.S. Citizenship and Immigration Services, USCG, CBP, and ICE. We have additionally discussed with States the possibility of joint interoperability pilot projects. Although none have been finalized, I would, if confirmed, welcome further discussion on the effectiveness of such projects, to ensure we reach as broad a segment of the law enforcement community as possible.

36. 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. The Senate-passed immigration reform bill would require an "electronic exit system" to be deployed to all air and sea ports, and that a biometric exit system be deployed to the 30 largest international airports within 6 years of enactment.

a. If the Senate-passed bill is enacted, please describe how you would implement its overlapping exit system requirements.

Response: Currently, DHS does not have biometric capability on exit. In planning for a future system, we need to ensure we will not be placing a tremendous resource burden on both the public and private sectors. Based on models developed in 2008 that involved fingerprinting all departing foreign nationals, DHS estimated that such a program, were it to be implemented at airports alone, would cost between $3.4B and $6.2B over ten years.

S&T is partnering with CBP and the NIST to invest $22M to develop new approaches and plan evaluations of new technologies that would provide the ability to enhance entry and exit operations and capture biometrics at a significantly lower operational cost than the previous biometric technologies piloted.

b. If confirmed, what steps would you recommend DHS take to ensure that an exit component is deployed to the airports as soon as possible? What are the challenges faced in doing so?

Response: With the $22M investment, DHS is currently developing a test facility, which is scheduled to be completed in late 2013, in order to begin to test emerging biometric collection technologies, including facial recognition and iris technology, in an airport-like exit environment.

A primary challenge is that U.S. airports do not have specifically designed and designated exit areas for outgoing international passengers to wait prior to departure, nor do they have specific checkpoints through which an outgoing international passenger's departure is recorded by a government official, as is the case in many other countries.

With the transfer of entry-exit functions to CBP, my role if confirmed as Under Secretary will be to work with CBP and other stakeholders to ensure OBIM supports any biometric entry-exit solution that is identified and implemented

c. Do you believe that a biometric exit system is needed? Please explain your reasoning either for or against a biometric exit system.

Response: DHS is committed to implementing a biometric exit/entry solution when it is cost-effective, , and affordable to do so. While a biometric-based program may have some advantages, DHS has confidence in its biographic targeting, pre-arrival, entry screening, and enhanced biographic exit programs. In all environments (air, land, and sea), biometrics may be collected upon a traveler's arrival and checked immediately against watch lists. Numerous biographic-based checks are queried simultaneously and, in the air and sea environments, biographic-based checks are completed well before the traveler boards the aircraft or vessel. Finally, because of the significant improvements in DHS's enhanced biographic system over the last several years, the need for a biometric exit system has been called into question, particularly in light of the costs and infrastructure challenges.

d. Why do you believe the Department been unable to implement a biometric exit system to date despite a clear Congressional mandate to do so?

Response: A primary challenge is that U.S. airports do not have specifically designed and designated exit areas for outgoing international passengers to wait prior to departure, nor do they have specific checkpoints through which an outgoing international passenger's departure is recorded by a government official, as is the case in many other countries. Based on models developed in 2008 that involved fingerprinting all departing foreign nationals, DHS estimated that such a program, were it to be implemented at airports alone, would cost between $3.4B and $6.2B over ten years.

At the land border, the infrastructure challenges are more acute, with far fewer lanes serving departures from the United States than for admission, and many land border ports-of-entry have severe infrastructure restrictions on expansion, for geographical or environmental reasons.

37. Some have argued that the only logical place for the collection of exit biometric data at airports 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?

Response: While we have tested and examined many locations for biometric collection, a biometric exit program or requirement is only worth the investment if it provides a reasonable assurance of departure. The advancement of biometric technologies such as combination facial recognition and iris may provide opportunities for biometric collection inside the jetway instead of specifically at the gate, which still achieves the assurance of departure. DHS will be testing several such processes in a closed environment during the next few months, as the Secretary has reported to Congress.

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

Response: This will depend on the biometric technology ultimately selected for the program. Each provides different operational possibilities in terms of collection location.

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

Response: DHS would only seek to prevent departure in the most extreme cases such as extremely serious pending criminal charges against the individual or that the individual is a known or suspected terrorist on the "no fly" list. These same processes occurs today using biographic information provided by the carriers prior to departure. A biometric exit program, with reasonable assurance of departure, would assist law enforement with a more accurate determination of whether non-U.S. citizens have departed the United States on time or remain in the country illegally

38. 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?

Response: At the land border, the infrastructure challenges are acute, with far fewer lanes serving departures from the United States than for admission, and many land border ports-of-entry have severe infrastructure restrictions on expansion, for geographical or environmental reasons. That said, DHS is committed to implementing a biometric solution when it is cost-effective, efficient, and affordable to do so.

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

Response: As an action item supporting President Obama and Prime Minister Harper's 2011 Beyond the Border initiative Plan, Canada and the United States agreed to exchange

land entry records at common, automated land ports of entry such that an entry record into one country serves as an exit record for the other. We are currently exchanging biographic information on third country nationals (including permanent residents) and are committed to expand to include exchange of data on all travelers (including citizens of both countries) in Summer 2014. The Department continues to explore options with Mexico to collect exit data on the Southern border.

39. 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?

Response: The agreements signed with Visa Waiver Program countries produce actionable law enforcement information that helps DHS officials identify individuals of interest at our ports of entry and in the interior. DHS, the FBI, and the Terrorist Screening Center have developed procedures for incorporating that information into border operations while adhering to the privacy controls contained in the agreements and standard protocols that set thresholds for law enforcement actions.

Emergency Communications

40. Meeting immediate and long-term emergency communications needs requires careful coordination among numerous federal agencies, including DHS, the Department of Commerce, and the Federal Communications Commission. This coordination will be all the more vital over the next decade as federal officials take on the task of building out a nationwide, interoperable, public safety network under the governance of FirstNet, the executive body responsible for laying the foundation for this network. In your experience, what is the key to a successful interagency effort involving numerous stakeholders? How has the FirstNet Board fared so far in its endeavor to facilitate coordination among its membership?

Response: Establishing open communications channels, a culture of trust, and a shared mission has been the key to the Department's past efforts for coordination across agencies, sectors and levels of government. Ensuring appropriate transparency in activities and engaging stakeholder groups create the required foundation for this exceedingly complex project of deploying FirstNet.

The challenge of planning, constructing, and deploying a Nationwide Public Safety Broadband Network is immense. The composition of the FirstNet board, as outlined by Congress, is intended to provide a cross-cutting representation of the stakeholders necessary to make the Nationwide Network successful. To date, the Board has met those expectations and continues to move forward on the network. The urgency by which FirstNet operates and the challenge of the mission and goals will create some challenges on their path toward deployment, though the maturation is already advancing significantly and there is a strong shared sense of the importance of this mission. FirstNet is also building on the successes previously established through NPPD

by leveraging State data collection efforts from our Office of Emergency Communications (OEC) Technical Assistance program, best practices from the Statewide Communications Interoperability Plan Workshops and well as existing partnership efforts such as the Emergency Communications Preparedness Center designation as primary body for federal consultation on FirstNet initiatives.

41. In 2012, the Department realigned functions of the former National Communications System within the Office of Emergency Communications. What efficiencies have been gained by this reorganization, and do you believe any additional realignment of emergency communications functions is needed within NPPD, or among DHS components?

Response: Implementation of EO 1361813618 resulted in the realignment of several functions from the former National Communications System into the Office of Emergency Communications. The result is a single entity with oversight and coordination of communications issues at all levels of government as well as the telecommunications industry. Currently, the OEC supports and promotes communications for emergency responders and government officials during all hazards and threats. The additional capabilities strengthen OEC and create more efficient coordination and exchange of information that is necessary to better address future challenges and opportunities, including emerging threats and advances in technology. At this time, there does not to appear to be a need for further realignment within NPPD or the Department, but DHS will continue to seek opportunities for additional efficiencies.

42. In passing the Post-Katrina Emergency Management Reform Act of 2006, Congress directed the Office of Emergency Communications to develop, and periodically update, a National Emergency Communications Plan to provide recommendations on emergency communications capabilities and interoperability for first responders and government officials in the event of natural disasters, acts of terrorism, and other man-made disasters. The first iteration of the National Emergency Communications Plan was released in July 2008. Since then, many new technologies have become available to first responders, and last year Congress passed legislation setting aside the D Block of broadband spectrum for a nationwide, interoperable, public safety network. What are your plans for updating the National Emergency Communications Plan to reflect these developments?

Response: OEC is in the process of updating the NECP to reflect first responders' use of new technologies during emergencies, including the deployment of the Nationwide Public Safety Broadband Network (NPSBN). OEC has been working with stakeholders from all levels of government and the private sector to develop the new NECP. DHS is targeting to release the updated Plan in early 2014.

43. DHS components operate several land mobile radio networks serving approximately 120,000 users. The Department has established a Department-wide Tactical Communications Network ("TacNet") program to develop an enterprise-wide approach to addressing the Department's tactical communications needs, supported by a Joint Wireless Program Management Office housed in Customs and Border Protection and

governed by an Executive Steering Committee. What should NPPD's role be in supporting the TacNet program?

Response: NPPD is one of three co-chairs of the Executive Steering Committee for the Joint Wireless Program Management Office. NPPD also provides governance coordination through the OneDHS Emergency Communications Committee, administered by OEC. The OneDHS Emergency Communications Committee brings together the policy and operational leaders from across the Department Components in order to provide feedback and guidance to the Joint Wireless Program Management Office. As one of the three co-chairs, NPPD is able to collect operational requirements from DHS components for the build out of FirstNet and contribute to interoperable communications on existing land mobile radio networks.

44. What interoperability challenges do the Wireless Priority Service and Government Emergency Telecommunications Service face in light of improvements in communications technology, like increased usage of Voice Over Internet Protocol ("VoIP")? If Next Generation Networks Priority Service is not fully funded in the upcoming years, how will you ensure the operational effectiveness of these services?

Response: NPPD is working diligently on next phases of the NGN priority services project. Through the National Security/Emergency Preparedness Executive Committee, and associated Joint Program Office, the Administration is working to define and designate capabilities that will ensure successful communications capabilities amongst and between key leaders at all levels of government during national-level crises and emergencies. The move to packet-based infrastructure provides both opportunities and new challenges to the interoperability of priority services. Commercial telecommunications providers, including those currently providing circuit-switched priority services, have already begun the replacement of their circuit-switched infrastructure with a higher capacity packet-switched infrastructure. Industry (including FCC) projections indicate that as early as 2015 but no later than 2018 circuit switched capacity will be insufficient to keep GETS operationally effective. Next Generation Networks (NGN) Priority Services programs are designed to provide voice-call priority in the service providers' commercial communications networks under all circumstances, including during periods of stress and significant outage/failure of network infrastructure. Reduced or limited funding of NGN Priority Services testing and deployment in conjunction with service provider transitions will cause a gap in those services currently available through GETS. DHS is also challenged with similar capabilities in data and video prioritization planning as those mediums become essential to operations under national emergency conditions.

Research & Development

45. What is the nature of NPPD's current research and development (R&D) portfolio? How do you plan to coordinate these efforts with the Science and Technology Directorate?

Response: A number of NPPD program offices currently coordinate projects with the S&T and other federal programs. We plan to continue to leverage S&T, the national labs, and FFRDCs in any future research endeavors.

V. Relations with Congress

46. 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?

Response: Yes.

47. 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?

Response: Yes.

VI. Assistance

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

Response: These answers are my own. I have consulted with staff in the Department for updates on various programs and projects, to inquire as to factual or historical information required to provide responses to certain questions, to confirm dates of events, and to properly cite any specific statutes or directives. I am responsible for the content of all responses.

I, Suzanne Spaulding, hereby state that I have read the foregoing Pre-hearing Questions and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

(Signature)

RANDOLPH SCOTT NOTARY PUBLIC DISTRICT OF COLUMBIA

District of Columbia: ss
Subscribed and Sworn to before me
this 17th day of September 2012
Randolph Scott Notary Public, D.C.
My Commission Expires June 30, 2014

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

Questions from Ranking Member, Senator Coburn

Policy Questions

Management

46. DHS, and in particular NPPD, has struggled with low employee morale, including during your time as a Deputy Under Secretary at NPPD. If confirmed, what will you change to improve morale at NPPD? Has NPPD conducted an analysis to determine the root cause of low employee morale within the Directorate? Will you?

Response: Through our analysis of the Employee Viewpoint Survey (EVS) results and other data, we have begun to implement a series of initiatives designed to address employee concerns and improve morale. Our employee input to the EVS surveys and feedback during brown bags, calls with our field forces, and other interactive sessions across the Directorate are some of the mechanisms we use inform our improvements to the workplace. In addition, we have implemented several new efforts to provide our staff with multiple outlets to express their views to senior leaders. Many of these engagements are bidirectional, giving leadership a chance to ask staff to assist the National Protection and Programs Directorate (NPPD) with improving the workplace environment and morale.

Based on feedback from our outreach efforts, we incorporated the leadership principles of accountability, professionalism, respect, integrity, communication and empowerment into our leader development programs and the employee on-boarding process. We also established an employee rotational assignment program and a mentor program to provide developmental opportunities to employees. Our senior leader performance plans include a mandatory performance objective that addresses improving employee satisfaction as identified through the Office of Personnel Management (OPM) Federal EVS.

To set expectations of the type of culture desired, we continue to improve our employee onboarding process and leader development programs. NPPD provides its leaders multiple training opportunities to enhance employee capabilities through the development of its basic and refresher supervisory courses as well as development of new leadership training for team leaders and team members. I have led the development of a series of performance management sessions where employees (supervisors and non-supervisors) are provided information on the

performance management process. My staff provides timely training during key times throughout the year but also provides ad hoc briefings when requested by individual organizations within NPPD.

I believe NPPD employees are the Directorate's most valuable asset. I hold each of my managers accountable to the leadership principles and encourage them to have an open door policy, listen to the feedback that they receive from their employees, and undertake efforts within their own organizations to continually improve organizational health. If confirmed, I look forward to continuing these efforts.

47. As Deputy Under Secretary for NPPD, what was your role in supervising the Directorate's production of Congressionally mandated reports? Has NPPD timely satisfied its duty to respond to Congressionally mandated reports during your time as Deputy Under Secretary and now Acting Under Secretary? What reports are currently overdue from NPPD and why?

Response: As Acting Under Secretary, I am responsible for ensuring that these reports are drafted and submitted in a timely manner. Congressionally-mandated reports are managed through the Office of the Chief of Staff. NPPD coordinates the preparation of reports with DHS's Office of the Chief Financial Officer as well as the Department's Executive Secretariat. NPPD has improved how it meets these requirements by assigning a dedicated reports manager and updating its tracking process. In the past year NPPD has increased its on-time submission rate by 30 percent. Currently, NPPD has three overdue reports. They are:

- Cyber Education and Workforce Development Plan for Veterans, Fiscal Year 2013—this report is currently undergoing Departmental review.
- Cyber Education and Digital Literacy Report, Fiscal Year 2012—this report is currently undergoing Departmental review.
- Annual Report on the Integrated Entry and Exit Data System, Fiscal Years 2010-2012—this report is currently undergoing Departmental review.

I will continue to work to improve NPPD's responsiveness to Congressional requests.

48. For FY2014 the President's budget proposed a 36% increase in NPPD's management and administration budget, including more than doubling the number of Public Affairs positions. Please explain why this increase is necessary in the current budget climate and how this may affect other areas within NPPD.

Response: NPPD is requesting the increase to the Management and Administration (M&A) appropriation to provide NPPD with adequate mission support capabilities to keep pace with the growth of its programs. NPPD has seen its cadre of Federal employees grow from 664 employees in fiscal year (FY) 2008 to 3,170 Federal employees in FY 2013. Since FY 2008, NPPD's budget has grown from $902 million to $2,439 million in budget authority (after sequestration). This increase is largely due to the growth of NPPD's cybersecurity programs and

the addition of the Federal Protective Service. Despite this dramatic growth in mission, the M&A budget has not seen any increase other than that attributed to budget realignment.

The requested increase to M&A in FY 2014 will ensure critical functions (such as budgeting, financial management, information technology, human resources, etc.) have sufficient resources to support NPPD's infrastructure protection, cybersecurity, biometric identity management, and Federal facility protection missions. Specifically, the increase will have the following impacts on NPPD's programs:

- Decrease vacancy rates and increase onboarding time for new employees, allowing NPPD to more quickly fill critical cybersecurity and Congressionally-mandated law enforcement positions.
- Improve budget planning for and the financial execution of funds appropriated to NPPD to support significant programs such as the National Cybersecurity Protection System, Continuous Diagnostics and Mitigation, and the Office of Biometric Identity Management.
- Improve the efficiency of the management of NPPD's portfolio of facilities, vehicles, and information technology assets.
- Ensure effective privacy oversight and communication related to NPPD's growing cybersecurity programs.

In addition, the complexity and size of NPPD's mission has grown, requiring a larger and more comprehensive public outreach capability. NPPD's work increasingly relies on its partnership with the private sector and external stakeholders. To ensure that NPPD effectively reaches the public and its stakeholders to inform them about cybersecurity initiatives, resilience planning, or protective services, among other things, we have requested an increase for our public affairs office.

Critical Infrastructure Protection

49. In August 2013, the State Department decided to close and reduce hours at many embassies in Africa and Middle East due to the threat of possible terrorist attacks. What actions, if any, did NPPD take to inform owners and operators of critical infrastructure that had facilities or personnel in those regions? Do you view NPPD as having a responsibility to provide information to critical infrastructure owners and operators with facilities overseas in such a circumstance?

Response: NPPD does undertake efforts to provide information to its partners that own and operate overseas infrastructure that may be affected by a particular threat. While the Department of State's Overseas Security Advisory Council (OSAC) has primary responsibility for notifying facilities located overseas, NPPD has an important role in providing information to the U.S.-based headquarters of these global companies. During this particular threat, NPPD's Office of

Infrastructure Protection (IP) worked with its government partners, including the Department of State, to provide unclassified messages from OSAC to several entities. Additionally, the National Infrastructure Coordinating Center, the information and coordination hub of a national network dedicated to protecting critical infrastructure essential to the nation's security, health and safety, and economic vitality, released information developed by IP on the Homeland Security Information Network (HSIN). IP worked closely with DHS Office of Intelligence & Analysis to coordinate messaging to critical infrastructure owners and operators with facilities, personnel, or other business equities overseas.

In addition, DHS has used the Threat Engagement Working Group, established in collaboration with our critical infrastructure partners, to meet with cleared private sector experts to benefit from their expertise in helping the government assess intelligence and develop actionable alerts with effective mitigation measures that can be shared more broadly with affected critical infrastructure sectors. While OSAC continues to have the lead on overseas notifications, we are committed to ensuring that future threat information sharing is timely, coordinated and actionable.

Cybersecurity

50. How many private sector entities have CRADA agreements with NPPD for cyber security information sharing? Do all of these entities currently have access to seats on the NCCIC floor? If any of the entities do not have access to NCCIC, please explain why this is the case and whether NPPD can take steps to enable their participation.

Response:

The Cybersecurity Information Sharing and Collaboration Program (CISCP) is an important part of our outreach and coordination efforts with owners and operators of critical infrastructure. A total of 57 entities to date participate, comprised of major corporations and information sharing and analysis centers (ISACs). Participants in the CISCP program enter into Cooperative Research and Development Agreements (CRADAs) with the Department that govern the details of the information sharing relationship, including privacy and civil liberties protections. These entities represent many sectors of critical infrastructure, including Communications, IT, Finance, Energy, Transportation, and Nuclear. Most of these entities have executed the appendix to the CRADA that enables them to maintain representatives on the NCCIC floor, which in practice will provide those entities' analysts periodic access to the NCCIC in order to connect and work collaboratively with NCCIC analysts in threat detection/prevention and mitigation solutions development efforts, as well as in incident management coordination. Few have expressed an interest for permanent, full-time access to the NCCIC floor. DHS is currently coordinating with the Department of Defense to process security clearances for such entities, which would enable them to access the NCCIC floor.

51. If you had much greater flexibility to reallocate resources within NPPD's cyber security programs, are their programs that you would like to emphasize and expand to become more significant priorities for NPPD and the Department? Are there any programs within

NPPD's cyber security work that you think are less critical and could be deemphasized or eliminated?

Response:

Program flexibility has been a challenge under the current sequestration. NPPD has seen disruptions to our workforce, training, and private sector collaboration efforts at a time when cyber threats are growing and evolving at an alarming rate.

One key priority for NPPD is to ensure that the physical consequences of a cyber event are fully understood. I have overseen the development of a stronger analytic capability that would fill a much needed gap in our ability to protect critical infrastructure. Current capabilities focus on operational responses to cyber incidents and traditional analysis of physical consequences. Greater focus must be given to the larger trends in both cyberspace and the physical world. In addition, NPPD is working to develop stronger analytical capabilities to identify dependencies and consequences of major events affecting critical infrastructure. I am pleased that in 2014 we will begin utilizing advanced metrics to further evaluate the efficacy and performance of our important programs. These metrics will help us to determine which programs are performing effectively and which programs require alteration and improvement.

Federal Protective Service

52. What was the total cost of all FSA-related activities within NPPD since FPS was moved into NPPD, to include RAMP and MIST development as well as the cost of conducting FSAs? How many FSAs have been completed in that time?

Response: The RAMP program cost a total of $37.7M for development, deployment, and sustainment. Because RAMP was not meeting its requirements, the Federal Protective Service (FPS) moved to cancel the program, for a total cost avoidance of more than $14M. Development costs for Modified Infrastructure Survey Tool (MIST), in comparison, were $850K and the tool was delivered in a short time by partnering with NPPD's IP to leverage a proven assessment methodology called the Infrastructure Survey Tool. MIST is now fully deployed and FPS has completed 1,660 Facility Security Assessments (FSA), using MIST, since summer 2012.

53. What role did you play, if any, in overseeing development of the Federal Protective Service's (FPS) Risk Assessment and Management Program (RAMP) tool? Do you consider the Department's investment into developing RAMP to have been a worthwhile investment? If not, why was it not stopped earlier? If so, what benefits will taxpayers see from that investment?

Response: The Risk Assessment and Management Program (RAMP) had been canceled prior to my arrival at NPPD. In May 2011, the decision was made to cease development of the legacy application known as RAMP and to pursue a standalone assessment tool, in order to provide completed FSAs to customers. That decision has since been affirmed by the Department's Office of Inspector General (OIG), which found that the timing of the cancellation of the RAMP project saved approximately $14 million in taxpayer dollars.

Research & Development

54. What is NPPD's research and development (R&D) portfolio as of August 22, 2013? In your response, please include a list of all active R&D projects, including but not limited to a list of all engagements with any of the national labs, federally funded research and development centers, or university-based centers of excellence.

Response: A number of NPPD program offices currently coordinate projects with the DHS Science and Technology Directorate (S&T) and other federal programs. We plan to continue to leverage S&T, the national labs, and federally funded research and development centers, in any future research endeavors.

Current NPPD R&D engagements include:

- The Office of Cybersecurity and Communications (CS&C) is working with MITRE Corp. and Concurrent Technologies Corp. on a Content Filtering Test and Evaluation to evaluate the security and operational mission capability (usability) of existing cybersecurity systems that provide content filtering capabilities that neutralize malware. This effort does not attempt to identify cyber malware; it transforms file content into a format that is highly unlikely to contain malware. These systems are characterized by the phrase "pass known good content" vice the current signature based systems that "deny known bad."
- CS&C is engaged in three pilot efforts with the Department of Defense (DOD) Defense Information Systems Agency (DISA) as part of the DHS/DOD Cyber Accelerator Program. These projects include a pilot to demonstrate that applications and data can execute in the public cloud with resiliency and integrity; a pilot to demonstrate a means to verify if client users (or malware infected client computers) are performing actions that are risky or malicious to enterprise resource servers; and a pilot to demonstrate a means to protect data and Intellectual Property (IP) when operating in a Software as a Service (SaaS) hosted environment beyond the enterprise perimeter.
- CS&C also partners with national labs, federally funded research and development centers, or university-based centers of excellence to leverage their expertise related to core mission areas such as control systems security, analytics, etc.
- FPS, S&T, and the General Services Administration signed a joint Research and Development Strategic Plan in July 2013. One goal of this plan is to provide strategic guidance for the S&T enterprise in satisfying the needs of FPS and GSA in protecting and making resilient government facilities, employees and capabilities, and the public. The plan envisions the export of developed capabilities across the Government Facilities Sector.
- IP is currently working on several projects with S&T including:
    - A water system modeling, simulation and analysis project;
    - Ongoing research to identify further chemicals that might be candidates for inclusion on Chemical Facility Anti-Terrorism Standards (CFATS) Appendix A;

- Participation in the Commercial Facilities Sector Coordinating Council Research & Development Working Group to review old and establish new R&D efforts with the intent of creating a prioritization process;
- Developing an IP Science and Technology research and development plan, which will provide strategic guidance and identify R&D project opportunities for S&T to satisfy the mission-based operational needs of IP.
- Capstone Integrated Project Teams (IPTs). The Chemical Sector Specific Agency (SSA) is involved in two Capstone IPTs: Chemical/Biological and Infrastructure Protection. The Chemical SSA is a Co-Chair of the Sub-Chemical IPT. The SSA also participates on the Steering Committee of the Chemical Security Analysis Center. The SSA attends Center of Excellence project reviews and participates in other IPT reviews as appropriate. These initiatives are ongoing and have been for at least six months.

- IP leverages its relationship with Argonne National Laboratory (ANL) for analytical capabilities in support of the Regional Resilience Assessment Program (RRAP), Site Assistance Visits and Enhanced Critical Infrastructure Protection (ECIP) Security Surveys. ANL support includes research, modeling, economic impact analysis, Geospatial Information System analysis, supply chain analysis, statistical analysis, and product development. ANL also provides subject matter experts from applicable fields to participate in site visits and discussions with owners and operators to assist in the development of a more comprehensive understanding of regional and system wide resilience of the Nation's critical infrastructure. Idaho National Labs has also been leveraged with regard to the enhancement of IP's cybersecurity understanding and efforts.
- Homeland Security Studies and Analysis Institute is conducting a Peer Review on the CFATS Risk Tiering Methodologies. The purpose of this project is to perform an independent assessment and analysis of the methodologies used by DHS to help identify and rank (i.e. tier) chemical facilities that could present a high risk of significant adverse consequences if subjected to terrorist attack, compromise, infiltration, or exploitation.
- Characterizing Vulnerabilities to Disruption of Critical Infrastructure (National Defense Research Institute RAND) - The objective of the project is to identify and prioritize specific infrastructure elements, types, or locations vulnerable to natural disasters with the potential for severe consequences to national commerce and well-being. Identifying such infrastructure can guide the federal government in efforts to minimize the risk of disruptions and their consequences.

55. Has NPPD engaged with research from any of the Department's university-based Centers of Excellence? If so, please specify what work. What added value do you think the Centers of Excellence provide toward NPPD's mission?

Response: NPPD is engaged in various research and development efforts in conjunction with S&T and various Centers of Excellence. For instance, IP has partnered with the Department's Centers of Excellence to integrate storm surge modeling into the National Infrastructure

Simulation and Analysis Center's capabilities, and on FASCAT, a secure web based application that compiles important food and agriculture information for identification, evaluation, and prioritization of critical food and agricultural infrastructure. We also work closely with DHS S&T to develop innovative solutions to fulfill cybersecurity mission needs and address gaps. CS&C provides technical requirements which are incorporated into S&T decision processes for R&D. The products of this collaboration can further NPPD's cybersecurity mission of protecting federal civilian networks and enhancing the security and resilience of critical infrastructure.

Our work with S&T and the Centers of Excellence, gives NPPD an opportunity to engage with a community not readily accessible through other mechanisms. NPPD views the unique skill sets and perspectives contained within the academic community as a significant asset and one which furthers our overall mission of developing public-private partnerships in service of enhanced critical infrastructure security and resilience.

IV. Open Recommendations from the DHS Office of Inspector General

56. Attached as Appendix 1 is a list of open recommendations from the DHS Office of Inspector General for NPPD. Addressing each recommendation separately, please explain why the recommendation is still open and what you will do to close it.

Response: Please see attached.

57. Attached as Appendix 2 is a list of open recommendations from the Government Accountability Office about NPPD programs. Addressing each recommendation separately, please explain whether and how you plan to address them.

Response: Please see attached.

Open OIG Audit Recommendations and Status Updates

- Attached as Appendix 1 is a list of open recommendations from the DHS Office of Inspector General for NPPD. Addressing each recommendation separately, please explain why the recommendation is still open and what you will do to close it.

Number	Title	Recommendation	Response
06-07	A Review of Top Officials 3 Exercise	We recommend that the Executive Director of the Office of State and Local Government Coordination and Preparedness: Design an information management system for use in future exercises that allows participants to track and share information more openly and efficiently; and, standardize the format and methodology for collecting and reporting information.	**Closed**: This recommendation was transitioned to FEMA. On August 26, 2013, FEMA officials provided OIG with a demonstration of its WebEOC capabilities. The demonstration and associated briefing conveyed functionality to support the intent of this recommendation. OIG considers the recommendation resolved and closed. Official confirmation of closure was communicated via OIG memo dated August 29, 2013.

Number	Title	Recommendation	Response
10-94	U.S. Computer Emergency Readiness Team Makes Progress in Securing federal Cyberspace, but Challenges Remain	We recommend that the Under Secretary of NPPD require the Director of National Cyber Security Division (NCSD) to: Establish a consolidated, multiple classification level portal that can be accessed by the federal partners that includes real-time incident response related information and reports.	Open: The Department concurred with the recommendation and is working to implement is. Completion is dependent upon the completion of National Cybersecurity Protection System (NCPS) Information Sharing capabilities and services (also known as Block 2.2). Information Sharing capabilities will enhance the NCPS's ability to securely share information with multiple stakeholders. Information Sharing and Collaboration includes the NCPS Block 2.2 project that will provide a secure environment for sharing Cybersecurity information with a wide range of security operations and information sharing centers across Federal, state, local, tribal, private, and international boundaries. Funding for the NCPS Information Sharing began in Fiscal Year 2013 and is moving forward. NPPD is applying regular program and project reviews to ensure timeliness and efficient completion of the Block 2.2 effort.

Number	Title	Recommendation	Response
10-94	U.S. Computer Emergency Readiness Team Makes Progress in Securing federal Cyberspace, but Challenges Remain	We recommend that the Under Secretary of NPPD require the Director of NCSD to: Establish a capacity to share real time Einstein information with federal agencies partners to assist them in the analysis and mitigation of incidents.	**Open**: DHS has received appropriated funds for information sharing, and it has begun the planning efforts necessary to implement all elements of NCPS Information Sharing and is preparing for an Acquisition Decision E-2B review in second quarter FY 2014. The NCPS Information Sharing Initial Operating Capability will be achieved in FY15, Full Operational Capability in FY18. NCPS Information Sharing will address the other open recommendations issued in this report incrementally but the exact timeline is still being determined as the project progresses. In order to ensure the success of the projects and the closure of the Recommendations, NPPD will utilize our program review processes to identify any potential issues that may arise and enable the project team to efficiently and effectively reach the established milestones while keeping our stakeholders informed.

Number	Title	Recommendation	Response
11-68	Information Sharing On Foreign Nationals: Overseas Screening	We recommend that the Office of Policy, and U.S. Visitor and Immigrant Status Indicator Technology: Coordinate and work with the DHS people screening programs which collect biometrics to use US-VISIT IDENT for their biometric storage and matching requirements.	**Open - Resolved**: The Office of Biometric Identity Management (OBIM) is currently prepared for testing of the Transportation Worker Identification Credential (TWIC)/Automated Biometric Identifications System (IDENT) interface, and is awaiting action from the Transportation Security Administration (TSA). OBIM plans to support the onboarding of the Office of the Chief Security Officer (OCSO) to take advantage of the IDENT/IAFIS (Integrated Automated Fingerprint Identification System) interoperability pathway. The IDENT changes to support this onboarding effort are currently scheduled for deployment in November. OIG personnel stated on June 28, 2013, that OIG considers the recommendation open but resolved. This recommendation will be closed upon the completion of integrating TSA TWIC and DHS OCSO biometric information into IDENT.

Number	Title	Recommendation	Response
11-68	Information Sharing On Foreign Nationals: Overseas Screening	We recommend that the Office of Policy, and U.S. Visitor and Immigrant Status Indicator Technology: Work with other federal agencies to share biometrics of foreign nationals collected by those agencies with DHS US-VISIT IDENT.	**Open - Resolved**: Sharing biometrics between DHS IDENT and the Terrorist Identities Data Environment (TIDE) is currently a manual process. Technological enhancements are underway for the automated transmission of known or suspected terrorist biographic and biometric information from DHS to the National Counterterrorism Center for inclusion in TIDE. Through this automation process, enhancements will be provided directly to NCTC and subsequently made available to interagency screening stakeholders. OIG personnel stated on June 28, 2013, that the OIG considers the recommendation open but resolved. OBIM is collecting the required documentation to close the recommendation.
11-89	Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure	We recommend that the Assistant Secretary, Office of Cybersecurity and Communications (CS&C): Define its program areas' responsibilities, priorities, and goals based on cybersecurity policy and the results of the Cyberspace Policy Review, Quadrennial Homeland Security Review, and Bottom-Up Review.	**Open**: CS&C continues to integrate refined guidance and future planning as part of an overall strategic planning effort. CS&C divisions such as the Office of Emergency Communications and Stakeholder Engagement and Cyber Infrastructure Resilience are refining their strategic plans as the overall mission space continues to expand and in some instances converge technologies. The recommendations with the OIG Audit are interrelated and are being addressed as part of the overall strategic planning process. CS&C has

Number	Title	Recommendation	Response
11-89	Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure	We recommend that the Assistant Secretary, Office of CS&C: Ensure that each program area develops and implements strategic plans that are focused on the critical tasks necessary to support DHS' efforts to safeguard and secure cyberspace and protect critical infrastructures, with an emphasis on the IT and communications sectors.	consolidated responsibility for issues such as those spelled out in the OIG recommendation in the Enterprise Performance Management Office (EPMO) within the Office of the Assistant Secretary. The EPMO will ensure that current measures throughout CS&C align with the CS&C Strategic plan once completed, and will make any necessary adjustments to previous measures and develop new measures to ensure overall program effectiveness. EPMO's Performance, Metrics and Quality branch is working with CS&C goal and objective owners to ensure performance measures are appropriate and align to overarching requirements both internal and external to CS&C. This includes the continuous review and alignment of performance measures associated with the DHS strategic and management measures sets, the DHS Cybersecurity Mission Management Plan measures, and Comprehensive National Cybersecurity Initiative measures. As the CS&C strategic intent is solidified, a performance measurement gap analysis will be conducted to determine where new measures are
11-89	Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure	We recommend that the Assistant Secretary, Office of CS&C: Develop a comprehensive strategic implementation plan that defines its mission and priorities, identifies milestones, and is aligned with its program areas' responsibilities and plans to support DHS' overall mission to secure cyberspace and protect CIKR.	

Number	Title	Recommendation	Response
11-89	Planning, Management, and Systems Issues Hinder DHS' Efforts To Protect Cyberspace and the Nation's Cyber Infrastructure	We recommend that the Assistant Secretary, Office of CS&C: Develop and implement objective performance criteria and measures that can be used to track and evaluate the effectiveness of actions defined in its strategic implementation plan and used by management to assess CS&C's overall progress in attaining its strategic goals and milestones.	required and whether pre-existing measures can be retired.
12-21	The Preparedness Directorate's Anti-Deficiency Act Violations for Fiscal Year 2006 Shared Service Administrative Assessments	We recommend that the National Protection and Programs Directorate: Report the FY 2006 Preparedness Directorate Anti-Deficiency Act (ADA) violations that are not corrected to the President, Congress, and the DHS Secretary in compliance with ADA reporting requirements. For each violation, the report should include title and Treasury symbol (including fiscal year) of the appropriation account, the amount involved, the date the violation occurred, the name of the official responsible for the violation, the type of violation, and the primary reason or cause.	**Open - Resolved**: NPPD reviewed and analyzed FY 2006 obligations and expenditures to identify potential shared-service/ADA violations. NPPD is currently working with OIG to close this recommendation.

Number	Title	Recommendation	Response
12-21	The Preparedness Directorate's Anti-Deficiency Act Violations for Fiscal Year 2006 Shared Service Administrative Assessments	We recommend that the National Protection and Programs Directorate: Conduct reviews of NPPD's shared services transactions for FYs 2007 to 2010, and identify and report any ADA violations according to OMB Circular A-11.	Open - Resolved: During FY 2013, NPPD reviewed and analyzed shared service transactions for FYs 2007 – 2010. The analysis results and draft report are undergoing management review, and NPPD anticipates issuing a final report early in FY 2014.
12-100	Effects of a Security Lapse on FPS' Michigan Guard Services Contract	We recommend that the Director of the Federal Protective Service: Provide clear guidance on whose responsibility it is and the criteria for determining whether posts are clean and orderly and free of unauthorized items.	Open - Resolved: FPS is on track to complete the revision of Directive 15.9.1.3, Contract PSO Performance Monitoring, to incorporate these considerations into the post inspection process. For contract guards, FPS is also revising the Security Guard Information Manual that is incorporated into all guard service contracts, to better define roles and responsibilities and FPS' definition of "clean and orderly posts." The OIG has reviewed FPS' response and stated that this recommendations will remain open pending revision of FPS' Directive 15.9.1.3, Contract PSO Performance Monitoring and the Security Guard Informational Manual. Estimated completion date is anticipated in the first quarter FY 2014.

Number	Title	Recommendation	Response
12-111	US-VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities	We recommend that the Director, US-VISIT: Review data inconsistencies that we have provided to the US-VISIT office to determine if additional examples of biographic fraud exist beyond the two cases that it previously referred to ICE.	**Open - Resolved**: OBIM completed the review of data inconsistencies provided by OIG on April 25, 2013. CBP National Targeting Center (NTC) agreed to review the 10,791 biometric identities that were identified by OBIM as needing to be reviewed for identity fraud and processing errors. OIG considers the recommendation open but resolved. OBIM is collecting the required documentation to close the recommendation.
12-111	US-VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities	We recommend that the Director, US-VISIT: Provide information on individuals determined to be using multiple biographic identities to appropriate law enforcement entities for identity fraud resolution and possible inclusion on the biometric watch list so they are identifiable when entering the United States.	**Open - Resolved**: The results of the OBIM analysis were delivered to CBP NTC on May 17, 2013. CBP NTC will work with appropriate agencies to pursue suspected identity fraud. CBP will report the outcomes of their analysis to include legal actions, watchlist promotions, and error corrections for which OBIM will relay to OIG. OIG considers the recommendation open but resolved. OBIM is collecting the required documentation to close the recommendation
12-112	DHS Can Strengthen Its International Cybersecurity Programs	We recommend that the Under Secretary, NPPD: Develop a comprehensive strategic implementation plan that defines CS&C's mission and priorities, specific roles and responsibilities, and detailed milestones for supporting the requirements outlined in the President's Strategy.	**Open - Resolved**: CS&C has worked through the necessary organizational adjustments to conform to the overall realignment of activities within the Office. Divisions are continuing to develop. CS&C is also engaging at the interagency and international levels to ensure consistent and realistic strategy development that encompasses multiple external stakeholders. CS&C has dedicated staff-members that are able to focus on strategic planning while maintaining visibility on operational efforts across the Divisions. This will result in a strategy that is durable in dynamic environment.

Number	Title	Recommendation	Response
13-20	Independent Auditors' Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting	We recommend that NPPD: Further the development of the accounting infrastructure through the implementation of standardized processes.	Open: In FY 2013, NPPD began standardizing business processes across the subcomponents. In FY 2014, NPPD plans to (1) complete standardizing business processes across the entity and (2) verify and validate the effectiveness of the implementation to ensure all subcomponents adhere to the standard guidance.
13-20	Independent Auditors' Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting	We recommend that NPPD: Develop and implement policies and procedures to foster communication between NPPD's Office of Financial Management (OFM) and the program offices.	Open: In FY 2013, NPPD stood up an Internal Controls Board (ICB) with representation from each Subcomponent and management line of business to ensure collaboration and leadership commitment across the entity. The NPPD ICB provides oversight and guidance to remediate the conditions reported in the Assurance Statement, address the lack of standardized policies and procedures, and identify corrective actions to improve NPPD's performance in Department-wide financial metrics. Due to the success of the ICB, NPPD plans to reduce the severity of its entity level control material weakness on its FY 2012 Assurance Statement to a reportable condition on its FY 2013 Assurance Statement. NPPD plans to keep it as a reportable condition due to recommendation 16 that remains open.

Number	Title	Recommendation	Response
13-20	Independent Auditors' Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting	We recommend that NPPD: Develop and implement policies and procedures to facilitate communication between NPPD OFM and the accounting service provider.	**Open**: The NPPD Financial Reporting team designed standard operating procedures to enhance visibility over work performed by service providers, focused primarily on the CFO Certification, payroll reconciliation, and property reporting processes. NPPD plans to complete implementation of the procedures and verify the effectiveness of the operations in order to fully remediate this finding in FY 2014.
13-39	DHS Can Make Improvements to Secure Industrial Control Systems	We recommend that the Undersecretary, NPPD collaborate with Office of the Chief Information Officer to streamline Homeland Security Information Network (HSIN) portal to ensure that industrial control systems (ICS) cyber information is shared effectively.	**Open**: Efforts are ongoing to update HSIN in order to accommodate sharing of Cyber information. NPPD has collaborated with the DHS Office of the Chief Information Officer (CIO) in order to implement upgrades to the HSIN portal to allow for greater information sharing. Due to the sensitivity of the data, the process requires some very deliberate planning, certification and accreditation as outlined by the DHS CIO. Currently we expect to have an initial capability enabled by mid-year FY 2014.

Number	Title	Recommendation	Response
13-39	DHS Can Make Improvements to Secure Industrial Control Systems	We recommend that the Undersecretary, NPPD promote collaboration with Sector Specific Agencies and private sector owners/operators by communicating preliminary technical and onsite assessment results to address and mitigate potential security threats on ICS.	Open: NPPD continues to foster collaboration and information exchange amongst the many stakeholders involved in Industrial Control Systems operations. The NPPD Office of Cybersecurity and Communications is working closely with the Office of Infrastructure Protection to more efficiently achieve the goals of the Recommendation and CS&C is sharing information to the extent that the Protected Critical Infrastructure Information laws allow. NPPD will continue to expand upon our ability to exchange information securely and as rapidly as possible with our stakeholders. This effort is a specific priority within CS&C and the capabilities will continue to expand as methods of exchange are developed. The refinement of these capabilities will meet the goals of the Recommendations.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division modify Chemical Security Assessment Tools to capture facility data efficiently and ensure that the tools provide meaningful end products for industry users and ISCD.	**Open - Resolved**: Improving CSAT is one of ISCD's top priorities for FY 2013 and 2014. Based on input received to date from the regulated community, as well as internal ISCD users of the outputs of the CSAT applications, ISCD has identified a number of potential improvements that should help make all three of the primary CSAT applications (the Top-Screen, Security Vulnerability Assessment (SVA), and the Site Security Plan (SSP)) more user-friendly, more efficient, and more effective. In order to revalidate and formalize those suggestions for improving CSAT, as well as identify any additional potential improvements, ISCD launched a "CSAT re-engineering and optimization" effort in 2012. This effort was broken into four tasks: formally engage the regulated community to solicit industry feedback and increase stakeholder involvement and buy-in, refine and document the process model for the lifecycle of a facility submission, document functional requirements to address industry concerns and information technology (IT) architecture inefficiencies, and revise and implement the modified IT system. In its report, the OIG stated that it considers these actions to be responsive and considers this recommendation resolved, but open, pending receipt of documentation that the modified CSAT is implemented. NPPD expects to complete these actions in FY 2014.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division document engagement with Office of Infrastructure Protection and DHS regulatory and voluntary programs to identify and implement existing tools and processes that can be leveraged to make Top Screen, Security Vulnerability Assessments, and the Site Security Plan tools more efficient, effective, and easier to use for the CFATS Program.	**Open - Resolved**: In NPPD's 90-day response to the OIG report, NPPD provided OIG with numerous documents providing evidence of ISCD collaboration with other DHS regulatory and voluntary programs to identify and implement tools and processes that could be leveraged to make the Top-Screen, SVA, and SSP tools more efficient and effective. OIG recently acknowledged that these documents provided evidence of collaboration, however, the OIG stated that the documents do not demonstrate how such collaboration resulted in tangible improvements to the Top-Screen, SVA, and SSP tools and that the recommendation will remain open until such documentation is received. NPPD is reviewing OIG's response and will work with OIG to address this recommendation.
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division Provide evidence of how the revised long term Site Security Plan review process has reduced the Site Security Plan backlog for all tiers.	**Open - Resolved**: NPPD concurs with the recommendation and has provided statistical evidence to the OIG on the current SSP authorization, inspection, and approval rates which significantly exceeds the historical throughput of SSPs, demonstrating that the current updated SSP review process is reducing the SSP backlog. The OIG has indicated to NPPD that it considers these actions responsive to the intent of Recommendation 3, but that the recommendation will remain open pending OIG's receipt and analysis of monthly statistics on the number of authorizations, inspections, approvals, and outstanding SSPs through September 2013. NPPD intends to provide the OIG with this information following the conclusion of FY 2013 activities

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division define, develop, and implement processes and procedures for Compliance Inspections, and train CFATS personnel to conduct Compliance Inspections.	Open - Resolved: ISCD has developed an SOP for inspections of CFATS covered facilities, which defines the different types of inspections conducted by ISCD, enumerates roles and responsibilities related to inspections, and details processes and procedures for pre-inspection, inspection, and post-inspection activities. During the summer of 2012, all of ISCD's CFATS inspectors participated in one of five two-week training sessions on the new, documented ISCD inspection protocols. Many of the lessons taught during these two week sessions are applicable to Compliance Inspections. ISCD's is providing additional training, more specific to Compliance Inspections, to all Chemical Security inspectors prior to their beginning to conduct those inspections in September 2013. NPPD has provided a training schedule which includes the tentative dates for conducting inspector training on Compliance Inspections and milestones for the development of the training materials that will be used during that training. OIG has informed NPPD that OIG considers these actions responsive to the intent of Recommendation 4, but that the recommendation will remain open pending receipt of the training materials and actual implementation dates for Compliance Inspection training. NPPD expects to complete these activities in the fourth quarter of FY 2013, and will provide OIG evidence of their completion once completed.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division identify and implement a process to improve the timeliness of ISCD determinations for all facility submissions.	Open - Resolved: NPPD recognizes that responding to facility submissions in a timely fashion is important for the operation of the program and continues work to reduce response times. In its report, the OIG stated that it considers the actions described by NPPD in its response to be responsive to Recommendation 5 and considers this recommendation resolved, but open, pending receipt of monthly reports on ISCD response times to facility submissions for FY 2013. NPPD has provided OIG with a report containing the monthly response times to facility submissions for the months between October 2012 and May 2013 and intends to continue to provide reports containing monthly response times to OIG for the remainder of FY 2013.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division develop a strategy and implement a plan to address facility resubmissions and requests for redetermination as prescribed in the CFATS regulation.	Open - Resolved: NPPD has established draft procedures and policies for receiving, reviewing, and responding to facility resubmissions and requests for redeterminations. ISCD has also provided guidance to facilities on how to properly request a redetermination and file a resubmission, established criteria for how to effectively process the requests, and determined appropriate review and analysis channels. NPPD has provided OIG with some of the key milestones for finalizing the procedures and policies associated with these activities and will provide OIG with a copy of the finalized procedures. OIG has indicated to NPPD that these actions are responsive to the intent of the recommendation, but that the recommendation will remain open pending receipt of the final policies and procedures associated with requests for redeterminations. Expected completion of the final SOP is second quarter, FY 2014

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division limit funding for Personnel Surety Program vetting until the Office of Management and Budget has approved the program's Information Collection Request.	Open - Resolved: NPPD non-concurred with this recommendation. It fails to consider the various factors and constraints that influence how, when, and to whom funding for the CFATS Personnel Surety Program (PSP) is allocated. As NPPD has done in the past, we will continue to perform careful and deliberate analysis prior to the expenditure of any funds related to the PSP program and will only allocate funding when appropriate given all relevant factors. Once the Information Collection Request has been approved by OMB and names have been sent to TSA for vetting, NPPD will provide that documentation to OIG.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division Develop an action plan and guidance for implementing the Ammonium Nitrate Program, which incorporates lessons learned from CFATS Program challenges.	**Open - Resolved**: As a proposed regulatory program, the Ammonium Nitrate (AN) Security Program's development is guided in large part by the regulations and procedures set forth in the Administrative Procedure Act, the authorizing statute, and OMB guidance with respect to rulemaking activities. NPPD has been working within those parameters to develop a final rule and an action plan and guidance for implementation of the final rule. Throughout the rulemaking and planning process, ISCD has been evaluating lessons learned from the CFATS Program and incorporating them into the development of the AN Security Program rulemaking activities and implementation planning. NPPD provided OIG with the steps NPPD plans to take to publish and implement the AN Security Program regulations. OIG has informed NPPD that it considers these actions responsive to the intent of Recommendation 8, which nevertheless will remain open pending our receipt of quarterly status updates of the AN Security Program Action Plan.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division develop and implement a curriculum and timeline for training inspectors to perform both Ammonium Nitrate and CFATS Program duties and responsibilities.	Open - Resolved: NPPD has developed and provided to the OIG a New Chemical Inspector Training Work Plan which includes a listing of the modules planned as part of the training and a timeline for training development and implementation. The OIG recently informed NPPD that it believes these materials are partially responsive to the intent of this recommendation, but that the recommendation will remain open pending receipt of copies of the training curriculum. NPPD is currently reviewing this response from OIG and will work with OIG to ensure that this recommendation is met.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division develop a methodology and reporting process to identify and address errors and anomalies that arise in the CFATS tiering methodology and risk engine.	**Open - Resolved**: NPPD has undertaken a three-phased approach to review the tiering process. This three-phased approach will consist of (1) documenting all processes and procedures relating to the tiering methodology, (2) conducting an internal DHS review of the complete tiering process, and (3) conducting an external peer review of the tiering methodology. The first two phases were completed by NPPD in 2012. The third phase is nearing completion. In addition to this formal review, the SVA and SSP review processes have been developed in a manner that requires multiple subject matter expert (SME) reviews of facility submissions. If at any point a SME identifies a potential anomaly in a facility's tiering, that anomaly is investigated to determine if it was a facility data error, an error within the tiering engine or risk methodology, or not an anomaly at all. ISCD is taking steps, delineated in a table provided to OIG, to formalize this process. NPPD expects to complete the development of the formalized process for documenting, reporting, and resolving potential anomalies within the risk engine by the end of FY 13, and will provide the OIG with a copy of that process once finalized. OIG has informed NPPD that it considers these actions responsive to the intent of Recommendation 12, but that the recommendation will remain open pending OIG's receipt of the finalized process for documenting, reporting, and resolving potential anomalies within the risk engine.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division provide the external peer review results, including comments on the V Factor, and ISCD's action plan to implement external peer review recommendations.	**Open - Resolved**: NPPD will provide OIG with a copy of the external peer review results, but cannot commit to implementing the peer review until the Department has reviewed the recommendations. NPPD provided key milestones to OIG regarding the completion of the peer review and ISCD's plans to address the recommendations by the second quarter of FY 2014. OIG has informed NPPD that it considers these actions responsive to the intent of Recommendation 13, but that the recommendation will remain open pending OIG's receipt of the peer review results and ISCD's plans with timeframes to address the review's recommendations.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division develop and implement a learning curriculum that (1) describes position roles and responsibilities clearly; (2) provides comprehensive training plans to prepare employees to perform assigned duties; and (3) communicates measures to assess performance.	**Open - Resolved**: In 2012, ISCD conducted human resources planning to determine and identify the human resources and the necessary skill sets required for program success. Using this and other information as a baseline, as well as a workforce analysis methodology, ISCD is developing a Human Resource Plan, which will include a staffing management plan and identification of training needs for all staff. Following the completion of the Human Resources Plan, ISCD intends to develop and disseminate an ISCD Employee Handbook that describes various aspects of the Human Resources Plan to all employees by the first quarter of FY 2015. OIG has informed NPPD that it considers these actions responsive to the intent of Recommendation 15, but that the recommendation will remain open pending OIG's receipt of documentation that the ISCD Employee Handbook has been developed and disseminated to all ISCD employees.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of NPPD's Office of Human Capital ensure that all employees receive performance reviews according to NPPD's General Instruction Guide on performance management.	**Open - Resolved**: On December 31, 2012, NPPD's Employee and Labor Relations Office issued a memorandum requiring subcomponent Chiefs of Staff to document and validate dates each employee signed a progress review by using the NPPD Performance Plan and Appraisal Report Certification (PPARC). Reports were submitted to NPPD by IP on behalf of all of its Division's for progress reviews by March 15, 2013, and were submitted for close-out reviews with summary ratings in 2013. Going forward, ISCD, via IP, intends to use the PPARC to track ISCD's completion of all required performance reviews. NPPD provided a copy of the NPPD PPARC Certification Form and the ISCD Performance Management Tracker, which was provided by ISCD to IP to allow IP to complete the IP wide PPARC. The ISCD Performance Management Tracker contains the dates upon which progress reviews were completed for each member of ISCD's staff. At this time, all current, non-SES ISCD employees have approved performance plans and received their progress review. In addition, in the fourth quarter of FY 2013, NPPD officials said they will provide an updated ISCD Performance Management Tracker demonstrating completion of all closeout reviews. OIG recently informed NPPD that it considers these actions responsive to the intent of Recommendation 18, but that the recommendation will remain open pending OIG's receipt of documentation demonstrating that all ISCD employees have received closeout performance reviews.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division eliminate the authorization and payment of Administratively Uncontrollable Overtime for all ISCD personnel.	**Open - Resolved**: NPPD does not concur with this recommendation. Instead of eliminating Administratively Uncontrollable Overtime (AUO), NPPD leadership has determined that the more appropriate path is to continue to permit CFATS Chemical Security Inspectors to claim AUO in a manner that is consistent with AUO rules and regulations, and that is supported by greater oversight, increased training, documented policies and procedures, and greater management controls. NPPD officials intend to provide OIG with the results of the AUO audit performed on ISCD personnel planned for the first quarter of FY 2014. OIG considers these actions partially responsive to this recommendation, but continues to question the need for AUO. OIG has indicated to NPPD that the recommendation will remain open pending OIG's receipt of documentation that demonstrate AUO payments to inspectors are supported and justified by current and long-term activities across multiple fiscal years.

Number	Title	Recommendation	Response
13-55	Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program	We recommend that the Director of the Infrastructure Security Compliance Division Improve the clarity of guidance provided to the CFATS regulated industry so that it can benefit from regular and timely comments on facility submissions.	**Open - Resolved**: NPPD intends to update guidance materials for the Top-Screen, SVA, and SSP. NPPD is also in the process of developing updated guidance related to its Chemical-terrorism Vulnerability Information (CVI) program, and intends to release guidance specific to the CFATS Personnel Surety Program when the CFATS Personnel Surety Program is launched. ISCD continues to routinely update its website and guidance material contained therein based on user feedback to provide clear guidance and assistance to the regulated community. NPPD officials also provided milestones for completing the updated guidance materials for the CSAT Top-Screen, SVA, SSP, CVI program, and the CFATS Personnel Surety Program by the end of FY 2014. OIG considers these actions responsive to the intent of Recommendation 24; however, the recommendation will remain open pending OIG's receipt of guidance materials for the Top-Screen, SVA, SSP, CVI program, and the CFATS Personnel Surety Program.
13-95	DHS Can Take Actions to Address Its Cybersecurity Responsibilities	We recommend that the Acting Assistant Secretary, CS&C: Coordinate with OMB to develop a strategic implementation plan, which identifies long-term goals and milestones, for Federal agency Federal Information Security Management Act compliance.	**Open**: CS&C's Federal Network Resilience (FNR) division is coordinating with OMB and through the interagency Joint Continuous Monitoring Working Group to finalize a FISMA strategic approach which aligns to FNR's Continuous Diagnostics and Mitigation (CDM) program.

Number	Title	Recommendation	Response
13-95	DHS Can Take Actions to Address Its Cybersecurity Responsibilities	We recommend that the Acting Assistant Secretary, CS&C: Update and finalize internal operating procedures and guidance documents to ensure that cyber responsibilities and procedures are clearly defined.	**Open:** CS&C's Federal Network Resilience (FNR) division has a final and signed set of internal procedural and guidance documents. The Cybersecurity Performance Management Operations Guide is in final draft awaiting signature and shared under a separate cover.
13-95	DHS Can Take Actions to Address Its Cybersecurity Responsibilities	We recommend that the Acting Assistant Secretary, CS&C: Improve communication and coordination with Federal agencies by providing additional clarity regarding the FISMA reporting metrics.	**Open:** CS&C's FNR division is finalizing the Cybersecurity Performance Management Operations guide which includes the following: (a) stakeholder awareness matrix that outlines communication activities; (b) service descriptions to include procedures, practices, and expectations for collaboration with and support to Federal agencies; and (c) an impact matrix that identifies specific criteria for assessing the quality of a question.
13-95	DHS Can Take Actions to Address Its Cybersecurity Responsibilities	We recommend that the Acting Assistant Secretary, CS&C: Implement a process to analyze and provide detailed feedback to Federal agencies concerning monthly vulnerability data feeds.	**Open:** The Federal Network Resilience Cybersecurity Performance Management branch has initiated a chartered project that will deliver a Transition Plan that will identify the tasks and activities involved in moving from the current Cyberscope data feeds to the CDM dashboard

Number	Title	Recommendation	Response
13-95	DHS Can Take Actions to Address Its Cybersecurity Responsibilities	We recommend that the Acting Assistant Secretary, CS&C: Establish a process to ensure that all CyberScope contractor system administrators have received adequate security training in compliance with applicable DHS, Office of Management and Budget, and National Institute of Standards and Technology guidance.	**Open:** CS&C's National Security Deployment (NSD) branch has developed a tracking mechanism that contains a list of all NSD contract support personnel as well as the dates of their security awareness training, privileged user training, and any industry certifications or degrees (e.g. CISSP, Security+, etc.).
13-95	DHS Can Take Actions to Address Its Cybersecurity Responsibilities	We recommend that the Acting Assistant Secretary, CS&C: Implement all required DHS baseline configuration settings on the CyberScope database	**Open:** CS&C provided documentation to support the OIG scanning and configuration findings of the CyberScope system. CS&C's NSD branch has provided the appropriate security baseline scanning profiles to the Data Center 2 (DC2) Vulnerability Assessment Team (VAT). The DC2 VAT stores the results of these scans on the DC2 SharePoint site.

Open GAO Recommendations and Status Updates

1. Attached as Appendix 2 is a list of open recommendations from the Government Accountability Office about NPPD programs. Addressing each recommendation separately, please explain whether and how you plan to address them.

Report Number	Audit title	Recommendation	Response

Report Number	Audit title	Recommendation	Response
13-353	Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened	To better assess risk associated with facilities that use, process, or store chemicals of interest consistent with the NIPP and the CFATS rule, the Secretary of Homeland Security should direct the Under Secretary for National Protection and Programs Directorate (NPPD), the Assistant Secretary for NIPP's Office of Infrastructure Protection (IP), and Dircetor of ISCD to develop a plan, with timeframes and milestones, that incorporates the results of the various efforts to fully address each of the components of risk and take associated actions where appropriate to enhance ISCD's risk assessment approach consistent with the NIPP and the CFATS rule.	As GAO noted in its report, the Department is taking a number of steps to review its current risk methodology and ensure that all three traditional security risk factors (i.e., consequence, vulnerability, and threat) are appropriately considered in the overall CFATS risk-based process. These steps include documenting all processes and procedures related to the tiering methodology, conducting an internal DHS review of the complete tiering methodology, conducting an external peer review of the tiering methodology, and engaging Sandia National Laboratories (SNL) to assist the Department in developing a model for identifying and tiering high-risk chemical facilities on the basis of economic consequences. The Department will use the results of these efforts to improve the CFATS tiering model, as appropriate, by developing an integrated plan with timeframes and milestones. DHS expects to develop the integrated plan by second quarter, fiscal year 2014, and expects to receive additional recommendations from SNL on incorporating economic consequence by third quarter, fiscal year 2014.

Report Number	Audit title	Recommendation	Response
13-353	Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened	To better assess risk associated with facilities that use, process, or store chemicals of interest consistent with the NIPP and the CFATS rule, the Secretary of Homeland Security should direct the Under Secretary for NPPD, the Assistant Secretary for IP, and Director of ISCD to conduct an independent peer review, after ISCD completes enhancements to its risk assessment approach, that fully validates and verifies ISCD's risk assessment approach consistent with the recommendations of the National Research Council of the National Academies.	Although the Department believes that the current external peer review will accomplish much of what GAO is recommending, the Department agrees that a second peer review is a worthwhile endeavor. DHS will develop milestones for completion following implementation of any changes to the tiering methodology based on the activities covered by Recommendation 1.
13-353	Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened	To enhance ISCD efforts to communicate and work with facilities, the Secretary of Homeland Security should direct the Under Secretary for NPPD, the Assistant Secretary for IP, and the Director of ISCD to explore opportunities and take action to systematically solicit and document feedback on facility outreach consistent with ISCD efforts to develop a strategic communication plan.	The Department is committed to exploring different opportunities to solicit and document feedback on outreach activities for the purpose of making CFATS-related outreach efforts more effective for all stakeholders. Expected completion, initiating approaches for systematically soliciting and documenting feedback on facility outreach, is fourth quarter, Fiscal Year 2013.

Report Number	Audit title	Recommendation	Response
13-11	Critical Infrastructure Protection: An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure	To allow for more efficient efforts to assess portwide resilience, the Secretary of Homeland Security should direct the Assistant Secretary of Infrastructure Protection and the Commandant of the Coast Guard to look for opportunities to collaborate to leverage existing tools and resources to conduct assessments of portwide resilience. In developing this approach, DHS should consider the use of data gathered through IP's voluntary assessments of port area critical infrastructure or regional RRAP assessments--taking into consideration the need to protect information collected voluntarily--as well as Coast Guard data gathered through its MSRAM assessments, and other tools used by the Coast Guard.	The Coast Guard and the NPPD Office of Infrastructure Protection will continue to work with the DHS Office of Resilience Policy on defining their role in the resilience of ports and contributing to this important function. The Office of Policy Resilience Integration Team (RIT) established a subcommittee in December 2012 to serve as a forum for discussing the harmonization of resilience activities and programs across DHS. Throughout 2013, the subcommittee held regular meetings to discuss methods for continuous cross-component collaboration regarding resilience.

Report Number	Audit title	Recommendation	Response
12-852	Critical Infrastructure: DHS Needs to Refocus Its Efforts to Lead the Government Facilities Sector	To enhance the effectiveness of the government facilities sector, the Secretary of DHS should direct the Federal Protective Service (FPS), in partnership with Office of Infrastructure Protection (IP) and Council members, to develop and publish an action plan that identifies sector priorities and the resources required to carry out these priorities. With consideration of FPS's resource constraints, this plan should address FPS's limited progress with implementing a risk management approach and developing effective partnerships within the sector. The plan should address, at a minimum, steps needed to: (1) develop appropriate data on critical government facilities; (2) develop or coordinate a sector-wide risk assessment; (3) identify effective metrics and performance data to track progress toward the sector's strategic goals; and (4) increase the participation of and define the roles of nonfederal Council members.	FPS is still actively engaging with sector partners to identify and implement a plan of action to address closure of this recommendation. To date, FPS has been working with the Government Facilities Sector Government Coordinating Council, the Interagency Security Committee, and the State, Local, Tribal, and Territorial Government Coordinating Council to identify and address cross-cutting issues for the Government Facilities Sector , while capitalizing on existing partnerships and coordination mechanisms among stakeholders. Milestones and planned completion dates were established for each of the steps, while considering FPS's resource constraints. It is important to note that successful implementation of the plan is contingent upon the voluntary participation of all sector partners. Expected completion date for the identified steps is fourth quarter, fiscal year 2014.

Report Number	Audit title	Recommendation	Response
GAO-12-378	Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments	To better ensure that DHS's efforts to promote security surveys and vulnerability assessments among high-priority CIKR are aligned with institutional goals, that the information gathered through these surveys and assessments meet the needs of stakeholders, and that DHS is positioned to know how these surveys and assessments could be improved, the Assistant Secretary for Infrastructure Protection. Department of Homeland Security, should consider the feasibility of expanding the follow-up program to gather and act upon data, as appropriate, on (1) security enhancements that are ongoing and planned that are attributable to DHS security surveys and vulnerability assessments and (2) factors, such as cost and perceptions of threat, that influence asset owner and operator decisions to make, or not make, enhancements based on the results of DHS security surveys and vulnerability assessments.	In June 2013, IP's Protective Security Coordination Division (PSCD) updated the 180-day and 365-day follow-up questions to more accurately capture all improvements to resilience (i.e., to include tracking of those that are ongoing and planned that are attributable to surveys and assessments). This update will be implemented during the next IST version update roll-out (typically January of each year). PSCD has determined such an update to be feasible, but the details of how it would be accomplished are still being resolved. Implementation ongoing.

Report Number	Audit title	Recommendation	Response
GAO-12-378	Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments	To better ensure that DHS's efforts to promote security surveys and vulnerability assessments among high-priority CIKR are aligned with institutional goals, that the information gathered through these surveys and assessments meet the needs of stakeholders, and that DHS is positioned to know how these surveys and assessments could be improved, the Assistant Secretary for Infrastructure Protection, Department of Homeland Security, should develop a road map with time frames and specific milestones for reviewing the information it gathers from asset owners and operators to determine if follow-up visits should remain at 180 days for security surveys and whether additional follow-ups are appropriate at intervals beyond the follow-ups initially performed.	In February 2013, IP finished analyzing and comparing the Site Assistance Visit 365-day and Enhanced Critical Infrastructure Protection Survey 180-day follow-up results. In April 2013, IP decided that no modifications will be made to the timelines for follow-ups at this time. This recommendation is considered implemented; pending closure by GAO.

Report Number	Audit title	Recommendation	Response
GAO-12-378	Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments	To better ensure that DHS's efforts to promote security surveys and vulnerability assessments among high-priority CIKR are aligned with institutional goals, that the information gathered through these surveys and assessments meet the needs of stakeholders, and that DHS is positioned to know how these surveys and assessments could be improved, the Assistant Secretary for Infrastructure Protection, Department of Homeland Security, should revise its plans to include when and how sector-specific agencies (SSAs) will be engaged in designing, testing, and implementing DHS's web-based tool to address and mitigate any SSA concerns that may arise before the tool is finalized.	The concept for sector-level view of assessment data has been proposed, and the requirements/feasibility of such a dashboard will be explored following completion of the owner and operator and State-level Web-based dashboards. When those are both complete, IP will meet with the SSAs to discuss developing a dashboard that they could use for their own risk management initiatives. Beyond the transition to a Web-based system for owner and operator dashboards, established milestones are premature at this point. Implementation pending.

Report Number	Audit title	Recommendation	Response
GAO-12-378	Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments	To better ensure that DHS's efforts to promote security surveys and vulnerability assessments among high-priority CIKR are aligned with institutional goals, that the information gathered through these surveys and assessments meet the needs of stakeholders, and that DHS is positioned to know how these surveys and assessments could be improved, the Assistant Secretary for Infrastructure Protection, Department of Homeland Security, should develop time frames and specific milestones for managing DHS's efforts to ensure the timely delivery of the results of security surveys and vulnerability assessments to asset owners and operators.	The deployment of the Web-based dashboards in February 2013 ensures timely delivery of the dashboards to owners and operators. The transition to Web-based delivery eliminates delays associated with the past practice of in-person delivery of the dashboards on DVD by Protective Security Advisors (e.g., availability of owners and operators, scheduling conflicts). Implemented; pending closure by GAO.

Report Number	Audit title	Recommendation	Response
GAO-12-378	Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments	To better ensure that DHS's efforts to promote security surveys and vulnerability assessments among high-priority CIKR are aligned with institutional goals, that the information gathered through these surveys and assessments meet the needs of stakeholders, and that DHS is positioned to know how these surveys and assessments could be improved, the Assistant Secretary for Infrastructure Protection, Department of Homeland Security, should design and implement a mechanism for systematically assessing why owners and operators of high-priority assets decline to participate and a develop a road map, with time frames and milestones, for completing this effort.	A tracking system will also be developed to capture the reasons why owners and operators decline ISTs and the ECIP Standard Operating Procedure will be updated to document the use of the new tool. The design of the tracking system for declinations was completed in June 2013. Implementation ongoing.

Report Number	Audit title	Recommendation	Response
GAO-12-378	Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments	To better ensure that DHS's efforts to promote security surveys and vulnerability assessments among high-priority CIKR are aligned with institutional goals, that the information gathered through these surveys and assessments meet the needs of stakeholders, and that DHS is positioned to know how these surveys and assessments could be improved, the Assistant Secretary for Infrastructure Protection, Department of Homeland Security, should institutionalize realistic performance goals for appropriate levels of participation in security surveys and vulnerability assessments by high-priority assets to measure how well DHS is achieving its goals.	IP is in the process of establishing metrics for all projects as part of the Balanced Scorecard Initiative and GPRA. This initiative recently began and implementation is ongoing.

Report Number	Audit title	Recommendation	Response
GAO-12-378	Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments	To better ensure that DHS's efforts to promote security surveys and vulnerability assessments among high-priority CIKR are aligned with institutional goals, that the information gathered through these surveys and assessments meet the needs of stakeholders, and that DHS is positioned to know how these surveys and assessments could be improved, the Assistant Secretary for Infrastructure Protection, Department of Homeland Security, should develop plans with milestones and time frames to resolve issues associated with data inconsistencies and matching data on the list of high-priority assets with data used to track the conduct of security surveys and vulnerability assessments.	IP addressed this issue in 2010 and 2011 with the assignment of unique numerical identifiers to each asset in the Linking Encrypted Network System assessment database and the National Critical Infrastructure Prioritization Program lists. Implemented; pending closure by GAO

Report Number	Audit title	Recommendation	Response
GAO 10-772	Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened	To better ensure that DHS's efforts to incorporate resiliency into its overall CIKR protection efforts are effective and completed in a timely and consistent fashion, the Assistant Secretary for Infrastructure Protection should develop performance measures to assess the extent to which asset owners and operators are taking actions to resolve resiliency gaps identified during the various vulnerability assessments.	IP developed performance metrics to determine the percent of facilities that planned, started, or implemented at least one security enhancement that raises the facility's Protective Measure Index or Resilience Measures Index score after receiving an Infrastructure Protection vulnerability assessment or survey. The measure shows the percent of facilities that have enhanced their security or resilience after receiving an IP vulnerability assessment or survey. Implementation expected first quarter, fiscal year 2014

Report Number	Audit title	Recommendation	Response
GAO 10-772	Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened	The Secretary of Homeland Security should assign responsibility to one or more organizations within DHS to determine the feasibility of overcoming barriers and developing an approach for disseminating information on resiliency practices to CIKR owners and operators within and across sectors.	The Department non-concurred with this recommendation as DHS already has a means to disseminate information to stakeholders. DHS shares a broad spectrum of information with partners through the coordinating councils, information sharing tools such as the Homeland Security Information Network - Critical Infrastructure, and through various mechanisms, such as the PSAs. As DHS's collection of data and knowledge of supply chains and interdependencies has grown through our assessments and other activities, DHS has begun to develop documents for our critical infrastructure protection partners that provide information on characteristics of critical infrastructure resilience. Implementation ongoing; expected completion: June 2014

Report Number	Audit title	Recommendation	Response
GAO 12-92	Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use	The Secretary of Homeland Security, in collaboration with the sector-specific agencies, sector coordinating councils, and the owners and operators of cyber-reliant critical infrastructure for the associated seven critical infrastructure sectors, should determine whether it is appropriate to have key cybersecurity guidance listed in sector plans or annual plans and adjust planning guidance accordingly to suggest the inclusion of such guidance in future plans.	NPPD is working closely with our NIST partners in the development of Cybersecurity Guidance provided to the critical infrastructure sectors. The NIST cyber framework draft has been released and the NPPD Integrated Task Force is working through the framework with the sector stakeholders for adoption of guidance and recommendations. NPPD will continue to support NIST in its development, implementation and the adoption of the Cybersecurity framework under EO 13636. NPPD is also supporting the owners and operators of the critical infrastructure as part of its ongoing IT SSA responsibilities and as a part of its responsibilities outlined in the Cybersecurity Executive Order. Implementation ongoing; working with GAO to close.

Report Number	Audit title	Recommendation	Response
13-275	Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts	To help assess efforts to secure communications networks and inform future investment and resource decisions, the Secretary of Homeland Security should direct the appropriate officials within DHS to collaborate with its public and private sector partners to develop, implement, and track sector outcome-oriented performance measures for cyber protection activities related to the nation's communications networks.	DHS has begun working with critical infrastructure sectors in partnership with NIST and has already identified initial sector-provided data points on current performance goal practices. DHS plans to use our engagements with critical infrastructure sectors and results from future NIST Cybersecurity Framework workshops to identify opportunities to encourage adoption of baseline performance goals. DHS intends to coordinate with public and private sectors to finalize baseline performance goals. DHS plans to coordinate with NIST to finalize the Cybersecurity Framework. DHS in collaboration with Sector Coordinating Council and Leadership Working Group plans to develop a draft outcome-oriented performance measures for cyber protection activities. The last step's expected completion is third quarter, fiscal year 2014.

Nominations Hearing on Suzanne E. Spaulding
To be Under Secretary for National Protection and Programs,
U.S. Department of Homeland Security
September 19, 2013

Post-Hearing Questions for the Record
Submitted to Ms. Suzanne E. Spaulding
From Senator Tom Coburn

Management

1. In your oral testimonies, both you and Mr. Bunnell stressed the value of a single, unified Department campus to improving employee morale. Mr. Bunnell, in particular said that his approach to management included "management by walking around." Yet, in your responses to the pre-hearing questions, you said that one of the programs you implemented to improve employee morale at the National Protection & Programs Directorate (NPPD) was a telework program.

   a. If having all employees at a single location is better for employee morale than distributing them across multiple locations, how would an employee telework program improve morale?

      Response:

      NPPD is committed to enhancing the welfare of our workforce. NPPD's telework program involves employees working from home on average 2-3 days every two-week period. Work-life balance has emerged as a high priority in past Federal Employee Viewpoint Surveys, and I feel strongly that offering our employees flexibility enhances their workplace satisfaction and empowers our workforce to be more productive as they work diligently to help secure our nation and preserve our way of life. At the same time, given the central importance of integrating programmatic activities across the Directorate, greater consolidation of our National Capital Region leased facilities would support NPPD's mission while also cultivating resource efficiencies and fostering employee morale. Moreover, the improved coordination from a consolidated facilities footprint would breed the trust and confidence that enables effective telework.

   b. How do you assure accountability and good communications with employees participating in the telework program?

      Response:

      In accordance with the Telework Enhancement Act of 2010, NPPD has devoted resources to developing an effective telework program. Leveraging technology platforms such as teleconferencing, iMessaging and video conferencing platforms, NPPD is working to assure accountability and promulgate effective communications across its workforce to

support productivity and collaboration. We remain committed to assuring accountability, including through signed telework agreements, and using technology to foster seamless communication with the workforce both in the traditional and mobile office environment. NPPD's investment in workplace mobility has resulted in industry and government awards for sustainability and return on investment, and empowers our workforce to be more productive and more engaged.

c. Have your broader efforts to improve employee morale been successful? What do you think the results from the next Federal Employee Viewpoint Survey will show?

Response:

I am committed to improving employee morale across the organization. Although culture change takes time, I believe we will ultimately make a difference by closely analyzing the results of the Federal Employee Viewpoint Survey (EVS) and by taking action when we receive feedback from brown bags, calls with our field forces, training sessions, offsites, and other interactive sessions across the Directorate.

Based on feedback from our outreach efforts, we incorporated the leadership principles of accountability, professionalism, respect, integrity, communication and empowerment into our leader development programs and the employee on-boarding process. We also established an employee rotational assignment program and a mentor program to provide developmental opportunities to employees.

NPPD provides its leaders with basic and refresher supervisory courses as well as development of new leadership training for team leaders and team members.

I believe NPPD employees are the Directorate's most valuable asset. I hold each of my managers accountable to the leadership principles and encourage them to have an open door policy, listen to the feedback that they receive from their employees, and undertake efforts within their own organizations to continually improve organizational health. I have also worked to ensure that each employee has a clear sense of NPPD's mission and how they fit into and support that mission. Providing these public servants with the tools they need to contribute to that mission is essential to improving morale. If confirmed, I look forward to continuing these efforts.

Cybersecurity

2. In your prehearing questions you said that the "Department's statutory authorities have not kept pace with evolving technologies and reliance on cyberspace by federal agencies and critical infrastructure," and you called for legislative action to correct that perceived deficiency. In your testimony you repeated that call, explaining that some federal departments and agencies disagree that the Department of Homeland Security's (DHS) has

clear authority in this domain.

a. Please provide a list of those departments and agencies to which you were referring.

Response:

A lack of explicit statutory authorization has delayed, and in some cases prevented, DHS from deploying the EINSTEIN system that is necessary to detect and prevent intrusions into Federal government networks. Other agencies in some cases have questioned how deployment of EINSTEIN under DHS authority interplays with their existing statutory restrictions on the use of agency data. For example, DHS has faced difficulty in deployment of the EINSTEIN system to some statistical agencies due to questions about the Confidential Information Protection and Statistical Efficiency Act.

As a result of this uncertainty, EINSTEIN has not been able to achieve 100 percent deployment. DHS and the Administration are seeking the statutory authorization that is needed to clarify this uncertainty and to enable agencies to disclose their network traffic to DHS for narrowly tailored purposes to protect agency networks, while making clear that Federal privacy protections for the data would remain in place. This certainty would permit DHS and participating agencies to ensure that all of the Government's most sensitive information is protected by the full range of capabilities available to protect Federal networks.

b. According to the attached memo (Attachment 1) and analysis from the Library of Congress's Congressional Research Service (CRS), DHS already has most of the statutory authorities it needs. Do you agree with the entirety of CRS's analysis? If not, with which parts do you disagree and why?

Response:

DHS agrees that existing authority provides a baseline to execute its core cybersecurity mission, including for protection of Federal networks and for incident response and mitigation activities. However, the Department executes this mission under an existing patchwork of statutory authorities, presidential directives and Executive Orders spanning multiple Administrations. The lack of clarity and difficulty of pinpointing DHS's authority to execute specific parts of its mission frequently causes uncertainty among DHS's mission partners, whether private sector entities or other executive agencies, and leads to delays in engaging with those partners. In addition to the EINSTEIN example discussed in the prior response, having a single clear expression of DHS cybersecurity authority would greatly enhance and speed up its ability to engage with affected private sector entities during a major cyber incident affecting critical infrastructure. DHS believes its authorities should be updated to better reflect its current cybersecurity responsibilities and ensure that DHS is able to more effectively and efficiently carry out that mission. If enacted, recent legislative proposals aimed at clarifying these existing

authorities and missions responsibilities would dramatically improve the cybersecurity posture of federal agencies and critical infrastructure.

3. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and Enhanced Communications Services (through the U.S. Cyber Emergency Response Team, US-CERT) provide cybersecurity advisories, alerts, and signatures/indicators to the public free of charge. Prior to NPPD's introduction of these services several companies in the private sector already offered similar services.

   a. What are the limitations to existing private sector cybersecurity advisory, alert, and signature/indicator services that NPPD seeks to fill through its provision of similar services? How do you and NPPD ensure that the services NPPD offers in issuing advisories, alerts, and signatures/indicators are limited to filling that unmet need?

      Response:

      NPPD's National Cybersecurity and Communications Integration Center (NCCIC) provides a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications incident integration for the Federal government, intelligence and law enforcement community, the private sector, and State, local, tribal, and territorial domains. Within the NCCIC, the US Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), are uniquely positioned at the intersection of the Federal government intelligence/law enforcement communities and the private sector owners of critical infrastructure. The NCCIC is the only entity that can combine classified intelligence and other unique Government information with information voluntarily reported to the Department by the private sector, in order to disseminate timely and actionable mitigation advice as broadly as possible to a full range of partners, including small and medium sized business and State, local, tribal, and territorial partners. The NCCIC also has access to unique government information and techniques that it is able to incorporate into programs like Enhanced Cybersecurity Services (ECS) to ensure that the information in ECS does not duplicate commercially available information.

   b. Generally, what policies or procedures does NPPD have in place to determine whether a proposed NPPD service or tool already exists in the private sector and prevent duplication or competition with those private sector services or tools? What documents would show those policies and procedures?

      Response:

      NPPD works closely with its partners to provide timely, actionable information on imminent or severe threats. Likewise, we encourage our partners to help us understand the potential impacts of threats, possible avenues for mitigating these threats, and any unmet requirements which may exist. These relationships also help us understand the security marketplace to determine where unique government resources can be better applied.

When designing a proposed service or tool for the private sector, NPPD works to ensure that it is incorporating unique government information or capabilities that are not available as commercial capabilities in the private sector, and that are widely disseminated to entities such as small and medium sized business or States and localities that may not otherwise be in a position to procure those services or capabilities. Moreover, in accordance with applicable directives, when DHS plans an acquisition the Department conducts industry days, market research, and other requirements to gain insight into existing private sector capabilities.

Critical Infrastructure Protection

4. In your responses to the questionnaire and during your testimony, you said that the CFATS Program had turned a corner, yet there is still much work to be done. Indeed, to their credit, NPPD leadership and staff have increased the pace of reviewing site security plans (SSPs) significantly over the past year; in the past three months alone the program has more than doubled the number of SSPs approved since the program's inception. According to the latest data, almost 300 SSPs have been approved, including a majority of the SSPs for highest risk (Tier 1) facilities.

   Nevertheless, approximately 91% of the 3,375 SSPs received have yet to be approved. Thus, one important area in which work remains to be done is continuing to accelerate the pace in reviewing SSPs. What will you do to improve the pace of reviewing SSPs?

   Response:

   While significant progress has been made over the last year as a result of the Department's commitment to advance the CFATS program, DHS recognizes that more can still be done to accelerate the approval process.

   One way the Department anticipates increasing the approval process is through the use of Alternative Security Programs. The Infrastructure Security Compliance Division (ISCD) has invested significant time and effort in working with industry groups to develop Alternative Security Program templates for use by their members. These templates will continue to enhance ISCD's ability to increase the pace of Security Plan approvals, particularly for corporations with multiple regulated sites. In parallel, ISCD has also taken steps to further increase its monthly Site Security Program and Alternative Security Program review capacity by allocating additional resources.

   In addition, ISCD has recently begun to implement key efforts to build upon and improve CFATS execution. Three key elements of the improvement efforts will specifically assist in reducing the remaining backlog of facilities:

   - *Chemical Security Assessment Tool (CSAT) Enhancements.* CSAT is the secure, web-based system ISCD uses to collect and analyze facility data for the CFATS program (e.g., Top-screen, SVA, SSP, etc.). ISCD is in the process of improving these tools to support more accurate data collection, which ISCD believes will further expedite the security

plan review process. The CSAT enhancements are projected to be completed by 4th quarter FY 2014.

- *Compliance Process Enhancements.* These include ongoing efforts to document operational requirements and procedures for the Top-screen, SVA, SSP, Inspection (non-cyber), Cyber Inspection, and Enforcement Processes and make improvements to increase efficiency and pace. In addition, the existing case management system is being replaced with a new case management system that will automate certain review and reporting tasks. This new system is expected to enter service during November 2013.

- *Tier 3 and Tier 4 Strategy.* Current ISCD milestones are focused on Tier 1 and Tier 2 facilities, and review and inspection processes have been developed with those highest risk facilities in mind. However, Tier 3 and Tier 4 facilities comprise the bulk of the regulated population. In order to complete the review and inspection of Tier 3 and 4 SSPs in a more acceptable time frame, alternative approaches to the current SSP review and inspection processes will be developed in collaboration with the regulated community. In addition to completing work on improving the suite of online tools through which top screens, Security Vulnerability Assessments and SSPs are submitted, ISCD will be working to develop streamlined procedures for authorization inspections and also will be working with stakeholders to build the next generation of ASP templates, using a "checklist" format that will lend itself to facilitating authorization/approval of security plans across broader segments of industry.

Collectively, these process enhancements will further enhance ISCD's ability to efficiently and effectively carryout its security plan review and inspection responsibilities.

5. One of the statistics you cited as evidence of the CFATS Program's success in increasing security at chemical facilities is that over 3,000 facilities have reduced their holdings of chemicals of interest (COIs) to below the screening threshold quantities. I am concerned that this statistic may be misleading—reflecting a shift of risk to outside the CFATS Program, rather than an actual increase in chemical site security. For example, facilities may be reducing COI holdings by increasing the frequency of COI shipments, which may increase risk to the public by increasing the number of opportunities for theft, sabotage, or accidental release along public throughways.

   a. What data does NPPD track, if any, on facilities that tier out of CFATS coverage as to why and how those facilities modified their holdings of COIs?

   b. What other quantitative metrics does NPPD maintain on the CFATS Program's success in increasing chemical facility security?

Response Part a:

Under 6 CFR 27.205(b), a covered facility previously determined to present a high level of security risk that has materially altered its operations may seek a redetermination of its high-risk designation. In addition, under 6 CFR 27.210(d), when a covered facility makes material

modifications to its operations or site, the facility is required to submit a revised Top-Screen. DHS thoroughly evaluates the information and documentation associated with any Request for Redetermination or Top-Screen re-submission to ascertain if the facility's high-risk status or tier should be modified. Additional information and documentation may include items such as shipping invoices and bills of lading. In certain instances, DHS may send inspectors onsite to obtain further information to enable DHS to fully evaluate the request for resubmission.

Response Part b:

NPPD, as part of current Government Performance and Results Act (GPRA) measures, continues to track implemented measures at CFATS regulated facilities as a measure of the program's success in increasing chemical facility security.

GPRA Measure Name: Percent of performance standards implemented by the highest risk chemical facilities and verified by DHS.

Measure Description:

"This measure reports the percent of applicable risk based performance standards (RBPS) that are approved and implemented within site security plans (SSPs) or alternative security programs (ASPs) for Tier 1 and Tier 2 facilities that are compliant with the Chemical Facility Anti-terrorism Standards (CFATS) regulation. Following submission of a proposed SSP/ASP by a covered facility, the CFATS regulatory authority will conduct an "authorization inspection" of the covered facility to verify that the SSP/ASP is compliant with the CFATS regulation. For this measure, SSPs/ASPs determined to meet the RBPS requirements with current and planned measures will be approved. Upon approval of its SSP/ASP, the covered facility is required to fully implement the existing measures that are described in the SSP/ASP."

Further, NPPD is working to expand upon its ability to track, and categorize, other performance standards highlighting CFATS successes across multiple areas to include, but not limited to, the implementation and/or installation of security measures to address detection capabilities, delay capabilities, response, mitigation, security management and cyber as part of Site Security Plans or Alternate Security Programs.

6. Only one year after CFATS was authorized, Congress authorized the Ammonium Nitrate Security Program (ANSP). Yet that program still remains in draft rulemaking stage.

   Why has it taken more than five years to implement a final rule for ANSP?

   Response:

   The Department has been hard at work developing a comprehensive Ammonium Nitrate Security Program regulation based on this statute. This work has included consultation with

Federal and State security partners with a vested interest in securing the sale or transfer of ammonium nitrate, as well as with many private sector stakeholders. The statute requires that sellers and purchasers of ammonium nitrate are vetted against the Terrorist Screening Database. The complexity of regulating the sale of ammonium nitrate necessitates an analysis of the threat caused by ammonium nitrate to determine what should be regulated under the Ammonium Nitrate Security Program and other options for mitigating the threat of ammonium nitrate. In addition, the complex composition of the potential regulated community (e.g., farmers, miners, etc.) warrants comprehensive evaluation prior to the Department's promulgation of a final rule. DHS held 12 public meetings during the 120-day comment period to brief the public on the proposed rule, listen to their concerns, and gather comments provided during those forums. The Department is evaluating the comments provided by the public, and is determining what responses will be appropriate to include in the final rule for the Ammonium Nitrate Security Program.

The Department is continuing to adjudicate comments received on the Ammonium Nitrate Security Program Notice of Proposed Rulemaking issued in August 2011 and is developing a final rule.

In 2010, NPPD completed a report on the threat of electromagnetic pulse (EMP) to our electric grid, specifically extra high voltage power transformers (EHVTs). Although the report is not public, according to your responses to the prehearing questions, the report documents EHVT and other electric grid component vulnerabilities to EMP, and makes specific recommendations to electric utilities to harden their systems against that threat. According to your staff, NPPD has done no more work on this issue since 2010, including surveying electric utilities to see if those recommendations were implemented.

If EHVTs' and other electric grid components' vulnerabilities to EMP were significant enough to warrant specific recommendations to utilities to harden against the EMP threat, why has NPPD not verified implementation of those recommendations in the intervening three years?

Response:

NPPD works with the Department of Energy, the Sector Specific Agency covering the electric grid, to understand a variety of threats, including electromagnetic pulse (EMP), as well as to develop recommendations to mitigate risks. NPPD's role related to the threat of EMP is assessing its effects in order to share information with partners so they can better understand and mitigate EMP risks. Following the development and publication of the report, NPPD worked through the voluntary framework established by the National Infrastructure Protection Plan (NIPP) to provide the report to private and public sector partners. The report was also posted on the Homeland Security Information Network (HSIN) for access by those with a need for the information.

Post-Hearing Questions for the Record
Submitted to Suzanne Spaulding
From Senator Kelly Ayotte

1. Is it possible to have a comprehensive cyber bill without strong information sharing and liability protections? How important do you believe buy-in and support from industry is for getting a strong bill passed through both bodies? Given that private sector owns roughly 85-90% of critical infrastructure, can their voice be marginalized?

Response:

The Administration and the Department both support the Congress moving forward with a comprehensive suite of legislation that facilitates cybersecurity information sharing between the government and the private sector as well as among private sector companies. We believe that such sharing can occur in ways that enhance privacy and civil liberties protections, reinforce the appropriate roles of civilian and intelligence agencies, and include targeted liability protections. Congress can support this effort by also pursuing legislation that provides DHS with the authorities we need to secure Federal civilian networks, protect critical infrastructure, respond to cyber threats, and combat cybercrime.

Industry input is vital to this process, which is why both the Department and the Administration have focused on dialogue and input from a variety of stakeholders. As an example, while working to implement the President's Executive Order on *Improving Critical Infrastructure Cybersecurity*, the Department began engagement with the private sector early in the process and conducted more than 100 working sessions, involving 1,100 attendees to ensure private sector partners were fully engaged. We have continued that engagement as implementation has progressed.

2. As you have been acting Under Secretary for NPPD, are there any problem areas you have identified that will require particular attention upon your confirmation? What will your priorities be?

Response: Though events can often dictate priorities, there are important initiatives at NPPD that I am eager to advance if confirmed. The CFATS program has steadily improved since I joined the Department as Deputy Under Secretary. While we implemented a series of programmatic and management reforms to improve the program, there is still much to be done. I pledge to continue the reforms we have instituted and work to make CFATS an efficient and effective chemical facilities security program.

The rapidly growing connection between physical and cyber infrastructure requires that we think about infrastructure protection holistically and understand the potential consequences of an attack across multiple critical infrastructure sectors. If confirmed, I plan to continue efforts underway to better integrate our cyber and physical activities and focus our resources on understanding consequences and measures to mitigate those consequences.

Building on the good work that NPPD is already doing, I pledge to strengthen relationships with our government partners and the private sector. Our Nation's security depends on strong public-private relationships. One of NPPD's most important missions is to build robust partnerships that will allow us to better serve the American people by increasing the security and resilience of the critical infrastructure upon which they rely.

Finally, none of these mission objectives can be accomplished without a capable and committed workforce. I will continue to make it a priority to empower the dedicated men and women at NPPD with a clear sense of mission and the tools they need to advance our important mission. In addition, we must continue to recruit the best and the brightest to build our capabilities to meet the challenges we face.

3. In your opinion, what are the most serious or imminent threats to the homeland that we face today? In other words, what must you be prepared for upon confirmation, and how are you prepared to face those threats?

Response: The Nation's critical infrastructure—which provides the essential services that underpin American society—is varied, complex, and decentralized. It is owned and operated by public and private sector entities under many different organizational structures, resulting in a large number and wide variety of stakeholders. It is also highly connected, with interdependencies between critical infrastructure assets, systems and sectors existing across geographic, functional and economic boundaries. The complexity and interconnectedness of our critical infrastructure is likely to continue increasing. This complexity and interconnectedness is mirrored in the kinds of events that threaten to disrupt that infrastructure, and in the cascading consequences of such a disruption. We must ensure our security and resilience measures also become more sophisticated and interconnected to address threats and hazards that stakeholders in various sectors have in common.

In NPPD, we are building an approach that strengthens security and resilience to acts of terror, natural disasters, and cyber incidents. We also recognize the inextricable linkage between physical and cyber critical infrastructure. And we do so while continuing to work closely with our partners in the critical infrastructure community to develop and implement measures that address the challenges they face.

ARNOLD & PORTER LLP

John B. Bellinger III
John.Bellinger@aporter.com
+1 202.942.6599
+1 202.942.5999 Fax
555 Twelfth Street, NW
Washington, DC 20004-1206

September 3, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland
Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland
Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Re: Nomination of Stevan E. Bunnell as General Counsel of DHS

Dear Chairman Carper and Ranking Member Coburn:

I am writing to support strongly President Obama's nomination of Stevan Bunnell to serve as General Counsel of the Department of Homeland Security.

I have known and worked closely with Steve for more than 15 years since we both worked as Counsel to the Assistant Attorney General for the Criminal Division of the Department of Justice in the late 1990s. I later served as Senior Associate Counsel to the President and Legal Adviser to the National Security Council in the White House from 2001-2005 and subsequently as The Legal Adviser (General Counsel) for the Department of State from 2005-2009, under Condoleezza Rice. I was involved in the creation of the Department of Homeland Security while I was at the White House, and I worked closely with previous General Counsels and senior officials of DHS on many difficult issues when I was at the State Department. As a result, I know both Steve and the requirements of the position to which he has been nominated.

Steve is a superb choice to serve as General Counsel of DHS. Indeed, while I know many lawyers in Washington, I cannot think of anyone better qualified for this position than Steve. He brings the combination of tremendous intellectual ability, extensive relevant government experience, managerial expertise in the government and private law practice, and great personal integrity and conscientiousness. If confirmed, he would be a uniquely valuable and trusted counselor for the new Secretary and senior officials of DHS as well as an excellent manager of the numerous lawyers in the General Counsel's office. Personally, I would sleep better at night knowing that Steve is advising the Secretary and senior DHS officials.

Prior to his current position as managing partner of the Washington office of O'Melveny & Myers, Steve served for more than 17 years as a career prosecutor in important positions in the Department of Justice, culminating in his service as Chief of the Criminal Division of the U.S. Attorney's Office for the District of Columbia, where he supervised a staff of 85 federal prosecutors working on complex and sensitive investigations. These positions have prepared him well for service as General Counsel of DHS. Steve was highly respected both for his own substantive expertise and as a manager of government lawyers. Steve also enjoys great respect in the legal community in Washington, including among many federal judges.

Steve is non-ideological, thoughtful, collegial, and unflappable -- all important qualities for service at DHS, a Department which must deal with many difficult and sensitive issues, often in crisis situations. Eleven years after its creation, DHS remains a work in progress. I am highly confident that, if confirmed, Steve will be able to strengthen both the General Counsel's office and the entire Department.

In sum, Steve Bunnell would be an outstanding General Counsel of DHS. I strongly urge the Committee, and the Senate, to approve his nomination as soon as possible.

Sincerely,

John B. Bellinger III

O'MELVENY & MYERS LLP

BEIJING
BRUSSELS
CENTURY CITY
HONG KONG
JAKARTA†
LONDON
LOS ANGELES
NEWPORT BEACH

1625 Eye Street, NW
Washington, D.C. 20006-4001

TELEPHONE (202) 383-5300
FACSIMILE (202) 383-5414
www.omm.com

NEW YORK
SAN FRANCISCO
SEOUL
SHANGHAI
SILICON VALLEY
SINGAPORE
TOKYO

WRITER'S DIRECT DIAL
(202) 383-5374

WRITER'S E-MAIL ADDRESS
lblalack@omm.com

September 10, 2013

VIA U.S. MAIL & ELECTRONIC DELIVERY

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

Re: *Nomination of Stevan E. Bunnell, Esq.*

Dear Chairman Carper & Ranking Member Coburn:

I am writing to endorse the nomination of my law partner Stevan E. Bunnell to serve as the General Counsel for the U.S. Department of Homeland Security ("DHS"). I have known Steve for nearly six years, both professionally and personally. He is a man of character and enormous integrity, and he is a lawyer of exceptional skill. As a former counsel for the Committee on Homeland Security and Governmental Affairs ("the Committee") and later the Chief Counsel and Staff Director of the Permanent Subcommittee on Investigations ("PSI"), I am confident that Steve will serve DHS with distinction.

Steve has been my law partner at O'Melveny & Myers since 2007. I have worked closely with him on a variety of high profile matters. His judgment and integrity are beyond question. Steve was so well regarded by his partners that he was asked to serve as head of our Washington, D.C. office after only a few years at the firm. This request was unprecedented and a testament to Steve's collegial and constructive management style. As the leader of the D.C. office, Steve demonstrated the uncanny ability to solve problems and manage difficult personalities in a fashion that left all participants feeling like their voices had been heard and their views considered. Steve is truly respected by every level of the office, whether it be his partners, associates or support staff. Steve honed these management skills as a senior attorney at

†In association with Tumbuan & Partners

the Office of the U.S. Attorney in the District of Columbia and at Main Justice, where he served as a career prosecutor for nearly two decades. Steve ultimately was appointed the Chief of the Criminal Division at the U.S. Attorney's Office and previously worked under the direction of Mike Chertoff on terrorism and homeland security matters, when Mr. Chertoff was the Assistant Attorney General of the Criminal Division early in the last decade. Steve understands government structures and processes and he knows how to manage them effectively. Based on my observation of Steve as a manager of lawyers both at the Justice Department and at O'Melveny & Myers, I have complete confidence in his ability to supervise and guide the legal function at DHS.

Fundamentally, however, I recommend Steve for this position because he is truly a "good-government", nonpartisan lawyer. I am a lawyer active in the affairs of the Republican Party and I previously served as counsel for the then - Republican Majority at the Committee. But, while I am sure Steve has partisan allegiances, as we all do, I cannot tell you precisely what they are. I have confidence that Steve will serve DHS with the goal of advancing the public good and only the public good. For all of these reasons, I hope that the Committee will favorably report his nomination to the full U.S. Senate for confirmation. And I welcome the opportunity to share with you or your staff my views regarding Steve should they be needed.

If you have any questions or require any further information from me regarding Steve's nomination, please contact me at your earliest convenience.

Very truly yours,

K. Lee Blalack, II

K. Lee Blalack, II

KLB:raf

Brian D. Boyle
1625 Eye Street, NW
Washington, D.C. 20006
Phone: (202) 383-5327

September 10, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Carper and Ranking Member Coburn:

Please allow me to take this opportunity to express unqualified support for the confirmation of Stevan Bunnell as General Counsel of the Department of Homeland Security.

I have known Steve professionally for over 25 years. We were introduced as a result of our clerking for the same U.S. Court of Appeals Judge (Laurence Silberman) in the late 1980s, crossed paths at the Department of Justice when I served as Principal Deputy Associate Attorney General in the Administration of George W. Bush, and had the pleasure of working together again when my colleagues and I were able to persuade Steve to join O'Melveny & Myers LLP as a partner. In recent years, O'Melveny has been fortunate to have Steve serve as Managing Partner of its Washington, D.C. office.

Based on these interactions with Steve, I can think of no one better suited—intellectually and temperamentally—for the position of General Counsel of Homeland Security. Steve quickly masters complex subject matters, has a practice of consulting with others and is inclusive in his decision making, and is a highly effective manager. His quiet competence, self-effacing manner, and generosity with colleagues inspire others to follow him. I urge the Committee to approve his nomination without delay.

Sincerely,

BRIAN D. BOYLE

September 4, 2013

The Honorable Thomas R. Carper
Chairman
Senate Homeland Security and Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Thomas A. Coburn
Ranking Member
Senate Homeland Security and Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Carper and Ranking Member Coburn:

I write in support of the confirmation of Stevan Bunnell for the position of General Counsel of the Department of Homeland Security

I have known Steve since we worked together when I was Assistant Attorney General for the Criminal Division of the Department of Justice and he served as my counsel. During his service with me, from 2001-2002, he made significant contributions in helping the department formulate the domestic response to the attacks of September 11th. That work gave Steve important insight into national security and counter terrorism issues, as well as other law enforcement matters.

After his service in Main Justice, Steve went on to senior positions at the United States Attorney's Office for the District of Columbia, culminating in the critical role of Chief of the Criminal Division of that office.

Again, that experience afforded Steve the opportunity to manage multiple high profile and challenging legal matters, including some with a national security element. Upon leaving government service, Steve continued his stellar career at a major national law firm managing its Washington D.C. office.

As former Secretary of Homeland Secretary I worked closely with our general counsel and understand the demands of that job. Steve Bunnell would bring an exceptional background to that position since much of the work of DHS involves dealing with law enforcement issues involving ICE, CPB, TSA, Secret Service, and Coast Guard. Steve's lengthy experience as a prosecutor prepares him to understand and address a wide variety of relevant legal questions. His

national security experience will stand him in good stead in dealing with the sensitive intelligence and counter terrorism problems that arise regularly at DHS. Finally, Steve in an experienced manager of attorneys which is a significant benefit in a job of general counsel.

I know Steve to be bright, even tempered, highly experienced and possessed of mature judgment. I am convinced he would serve the Department and the Nation well as DHS general counsel. I urge the committee and the Senate to swiftly approve his nomination.

Please contact me if I can be of any assistance.

Respectfully,

Michael Chertoff
(202) 552-5280
1399 New York Ave NW
Suite #900
Washington, D.C.
20005

O

O'MELVENY & MYERS LLP

BEIJING
BRUSSELS
CENTURY CITY
HONG KONG
JAKARTA†
LONDON
LOS ANGELES
NEWPORT BEACH

1625 Eye Street, NW
Washington, D.C. 20006-4001

TELEPHONE (202) 383-5300
FACSIMILE (202) 383-5414
www.omm.com

NEW YORK
SAN FRANCISCO
SEOUL
SHANGHAI
SILICON VALLEY
SINGAPORE
TOKYO

WRITER'S DIRECT DIAL
(202) 383-5388

WRITER'S E-MAIL ADDRESS
aculvahouse@omm.com

September 6, 2013

VIA FACSIMILE AND FIRST CLASS MAIL

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Re: ***Stevan E. Bunnell, Nominee for General Counsel, Department of Homeland Security***

Dear Chairman Carper and Ranking Member Coburn:

I write in support of the confirmation of Stevan E. Bunnell as General Counsel of the Department of Homeland Security.

Steve Bunnell is superbly qualified to be DHS General Counsel. For 17 years he was a career prosecutor, trial attorney and ultimately supervisor with the United States Attorney's Office in the District of Columbia (including as Chief of the Criminal Division, supervising 85 other Assistant U.S. Attorneys) and/or with the U.S. Justice Department's Criminal Division (including as Counsel to the Assistant Attorney General in both the Clinton and George W. Bush Administrations). While serving in those capacities, Steve received both the Attorney General's Special Commendation Award (1995) and the Department of Justice Special Achievement Award (eight years). I personally know from having recruited Steve to private practice in 2007, and working closely with him since, that Stevan Bunnell is immensely respected by federal judges and by a large and diverse array of current and former government prosecutors.

More recently, Steve Bunnell has practiced law as a partner at our firm, O'Melveny & Myers LLP, for almost eight years; he also has been the Managing Partner of our 110-attorney Washington Office since 2011. Our clients greatly value his legal skills, he enjoys the full

†In association with Tumbuan & Partners

confidence of his 200+ partners across 16 offices, and he is much admired by his attorney and staff colleagues as a thoughtful and fair administrator and as a professional role model.

Steve Bunnell views public service as an attorney's highest calling. He instinctively knows that integrity and candor are the true currency of our profession, and that our a government attorney's everyday job is to uphold the Constitution and Rule of Law. While serving as President Reagan's White House Counsel and on several government boards and commissions, the government lawyers I respected the most were those whose intellectual rigor and creativity were expressly grounded on the Constitution and statutory law and who carefully paid due deference to the relevant precedents and established Executive Branch opinions and policies, even when their advice was inconsistent with the "favored" outcome. Steadiness, taking the long view, and understanding that one's client is the United States are traits that a departmental general counsel must have.

Steve Bunnell is such a lawyer. He is expert and experienced; he calls them like he sees them; and, while a terrific advocate, he would not proffer strained, situationally convenient legal advice, that deviates from the plain meaning and established interpretations of applicable law, in order to support the preferred policies of the day.

If confirmed, Steve Bunnell will serve with great distinction and will honor his oath as an officer of the United States to support and defend our Constitution.

Yours respectfully,

Arthur B. Culvahouse, Jr.
O'MELVENY & MYERS LLP

ABC:jjn

OMM_US:71803286.1

ALICE S. FISHER
555 ELEVENTH STREET, N.W., SUITE 1000
WASHINGTON, D.C. 20004-1304
(202) 637-2232
alice.fisher@lw.com

September 18, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security
and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security
and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

Re: Stevan E. Bunnell, Nominee for General Counsel, Department of Homeland Security

Dear Chairman Carper and Ranking Member Coburn:

I submit this letter in strong support of Steve Bunnell's nomination to serve as the General Counsel of the Department of Homeland Security. I believe that Steve has the qualities, intellect and character to serve the country in this important position.

I worked with Steve while he was at the Department of Justice, Criminal Division and when he served in the U.S. Attorney's Office in the District of Columbia. He constantly demonstrated his commitment to the country and to public service. In the very harried days after the terrorist attacks of September 11, 2001, Steve worked tirelessly in the Criminal Division on a range of issues facing our nation. In every way, Steve brought calm, consistent judgment to the tasks at hand. He worked closely with the FBI and other federal agencies in a collaborative manner, again and again demonstrating something that will be highly important in his role as General Counsel of DHS where he will be working on a daily basis with agencies here and abroad on the important security issues.

Likewise, while Steve served as the Criminal Chief of the US Attorney's Office, I worked with him while I served as Assistant Attorney General of the Criminal Division on a range of criminal matters. He exhibited great judgment on matters and policy and always demonstrated a collaborative approach. He has expertise not only in law enforcement and security issues that will be important, but also substantive legal issues critical to this role. For example, Steve worked hard on the Department of Justice's Procurement Fraud Task Force and will bring a depth of experience in this area to his role in advising on DHS procurement issues. He also worked closely with many of state and federal law enforcement and investigatory agencies. I have no doubt that Steve is very well suited to provide smart, sound, legal counsel to DHS and all of the entities which form it.

I know Steve has the highest ethics and professionalism. If confirmed, he will be a wonderful asset and colleague to all at DHS. I thank you for allowing me to provide this letter for your consideration.

Sincerely,

Alice S. Fisher

Ivan K. Fong
Senior Vice President
Legal Affairs and General Counsel

3M Legal Affairs

3M Center, Bldg. 0220-14-W-07
St. Paul, MN 55144-1000
Phone: (651) 737-0770
Email: ifong@mmm.com

3M

September 25, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Carper and Ranking Member Coburn:

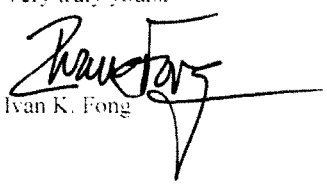
I am writing (in my personal capacity) to enthusiastically support Stevan Bunnell's nomination to serve as General Counsel, U.S. Department of Homeland Security (DHS).

I support Steve's nomination from two relevant perspectives. First, I have known Steve for over 25 years: He was a year ahead of me at Stanford Law School in the mid-1980s; we worked with each other on the *Stanford Law Review* then; and we have kept in touch with each other professionally and socially ever since. His experiences as a federal prosecutor, as counsel to the Assistant Attorney General for the Criminal Division, as chief of the Fraud and Public Corruption Section and later the Criminal Division of the U.S. Attorney's Office in Washington, DC, and now as managing partner of the Washington, DC office of the international law firm of O'Melveny & Myers make him an ideal candidate to serve as General Counsel of DHS. I have seen firsthand his commitment to professionalism, ethics, and mentorship when we were both members of the Edward Bennett Williams Inn of Court. Most important, his outstanding legal skills, strong reputation for integrity, and dedication to public service and the public interest give me great confidence that he would excel as the next General Counsel of DHS.

Second, as the most recent General Counsel of DHS (from May 2009 to October 2012), I believe I am in a unique position to evaluate and endorse Steve for this particular role. His extensive background in law enforcement and national security matters will prove to be indispensable to the critical role the General Counsel of DHS plays in assessing and recommending legal and policy solutions to the challenging issues DHS faces. In addition, Steve's substantial leadership and managerial experiences in the U.S. Attorney's Office and in private practice will be of immense value to him and to the Office of General Counsel at DHS.

In sum, Steve's legal ability, leadership experience, and personal qualities make him a first-rate nominee for the position of DHS General Counsel. I urge his prompt confirmation to this important position without reservation.

Very truly yours,



Ivan K. Fong

Shawn Henry
Former Executive Assistant Director, FBI
117 N. Park Dr.
Arlington VA 22203

September 5, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Carper and Ranking Member Coburn:

I recently retired as Executive Assistant Director of the FBI in March 2012, after 24 years of service. In that capacity, I was responsible for all FBI criminal investigations and cyber operations worldwide, as well as all FBI international operations and Critical Incident Response. I am writing today to provide my unqualified endorsement and recommendation for Steve Bunnell as General Counsel at the Department of Homeland Security. I have known Steve for more than 20 years, meeting him for the first time in 1990 when he was an Assistant United States Attorney in Washington DC and I was a rookie FBI agent.

Our careers have crossed many times for more than two decades, through his various positions at the United States' Attorney's Office and Department of Justice, and my ascension through the ranks at the FBI. I have observed Steve operate in various situations, and I have always been impressed by his intellect and thoughtfulness. My experiences in the FBI have taught me that investigators and prosecutors must collaborate throughout an investigation, as one law enforcement team. Steve has demonstrated that ability time and again. He routinely exhibits tremendous judgment, sincere deliberation, and outstanding problem solving skills, all in support of doing "the right thing."

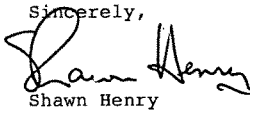
I have witnessed Steve's tireless efforts and commitment to seeking justice. I was a supervisor in the FBI's Public Corruption Unit in the mid-1990s and I worked routinely with the Public Integrity Section at DOJ where Steve was an attorney. We regularly had complex investigations with tight deadlines, unparalleled scrutiny, and extreme sensitivity. Steve investigated these matters with passion and intensity, and always exhibited integrity and professionalism.

The threats we face today are some of the most significant we have seen in our nation's history; terrorism, weapons of mass destruction, and cyber exploitation of critical infrastructure. As a former senior executive in federal law enforcement, I know very clearly the requirements and characteristics necessary to successfully meet and mitigate these threats. Steve Bunnell possesses not only the skills

and subject matter expertise required, but also the character and determination to succeed.

I have worked with thousands of government employees over the years, and Steve's commitment to the citizens he serves is the epitome of public service. It has been my honor and privilege to work with him over more than two decades, and I hope you will seriously consider him for this critical position. Thank you for your consideration, and I am available to answer any additional questions or concerns you may have.

Sincerely,



Shawn Henry

O'MELVENY & MYERS LLP

BEIJING
BRUSSELS
CENTURY CITY
HONG KONG
JAKARTA†
LONDON
LOS ANGELES
NEWPORT BEACH

1625 Eye Street, NW
Washington, D.C. 20006-4001
TELEPHONE (202) 383-5300
FACSIMILE (202) 383-5414
www.omm.com

NEW YORK
SAN FRANCISCO
SEOUL
SHANGHAI
SILICON VALLEY
SINGAPORE
TOKYO

WRITER'S DIRECT DIAL
(202) 383-5170

WRITER'S E-MAIL ADDRESS
tkassinger@omm.com

September 10, 2013

Via Regular Mail, Fax, and Email

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security
and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security
and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Carper and Ranking Member Coburn:

I am honored to write in support of President Obama's nomination of Stevan E. Bunnell to become General Counsel of the U.S. Department of Homeland Security. Mr. Bunnell is an exceptionally well-qualified candidate for this position.

From more than three decades of professional experience, including my service first as General Counsel and subsequently as Deputy Secretary of the U.S. Department of Commerce during 2001 - 2005, I am deeply familiar with the mission and responsibilities of the Department of Homeland Security, and the multiple roles that the General Counsel must play as public servant, lawyer, counselor, and administrator. The Department's next General Counsel will be tested by a broad range of complex challenges interweaving law enforcement, national security, regulatory, and business issues, often in a cross-border context.

Mr. Bunnell would bring to these challenges an abundance of intellect, professional skills experience, and remarkable personal qualities. For 17 years, he served in positions of increasing responsibility as a prosecutor and supervisor at the Department of Justice, including as Chief of the Fraud and Public Corruption Section, and as Chief of the Criminal Division in the U.S. Attorney's Office in Washington, D.C. His prosecutorial experience has been enriched by his equally impressive records of accomplishment in the private practice of law, both before and since his years at the Justice Department.

I have been privileged to work alongside Mr. Bunnell over the past six years as partners in the firm of O'Melveny & Myers. I know firsthand his integrity, commitment to the rule of

† In association with Tumbuan & Partners

law, dedication to our country's national security, and respect for individual freedom. Mr. Bunnell would serve our country with distinction, and I am pleased to commend his nomination to you with the utmost respect and enthusiasm.

Sincerely,

Theodore W. Kassinger

TWK:bah

David S. Kris
9825 SE 42nd Place
Mercer Island, WA 98040

September 1, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Carper and Ranking Member Coburn:

I write in strong support of the nomination of Stevan Bunnell to be General Counsel of the Department of Homeland Security.

I have known Steve for many years, as we have both worked at the Department of Justice at various times since the early 1990s. Steve has had a distinguished career in government and the private sector, as an Assistant U.S. Attorney, a member of the Criminal Division's Public Integrity Section, and a private law firm partner. He has policy and managerial experience, having served as Counsel to the Assistant Attorney General in the Criminal Division for both Jim Robinson (during the Clinton Administration) and Michael Chertoff (during the Bush Administration); today, Steve is the managing partner of the DC office of his law firm, O'Melveny & Myers. In his work in government, Steve has dealt with public corruption, terrorism, cyber issues, the USA PATRIOT Act, and related matters. Steve is very smart, very capable, and extremely respectful of the rule of law.

I urge the Senate to confirm Stevan Bunnell as General Counsel of the Department of Homeland Security.

Sincerely,

David S. Kris

Stuart A. Levey
36 Belsize Grove,NW3 4TR
London, UK

September 11, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Carper and Ranking Member Coburn:

I am writing in support of the nomination of Stevan Bunnell to be the General Counsel of the Department of Homeland Security.

I was the Under Secretary for Terrorism and Financial Intelligence at Treasury from 2004 until 2011, serving under both President Bush and President Obama. I am now the Chief Legal Officer of HSBC Holdings, plc, although I am writing this letter strictly in my personal capacity.

I have known Steve since my earliest days as a lawyer and our professional paths have overlapped in numerous ways over the past two decades. We both clerked for Judge Laurence Silberman on the United States District Court of Appeals for the District of Columbia Circuit, and we both worked for the criminal defense firm, Miller, Cassidy, Larroca & Lewin. Steve was a senior Department of Justice official when I worked in the Deputy Attorney General's office from 2001 until 2004. I have, therefore, had numerous opportunities to observe Steve's personal and professional conduct, and it gives me pleasure to offer my unmitigated support of Steve's nomination.

In all the years I have known him, I have found Steve to be an insightful and dedicated lawyer and a person of unquestioned integrity. He has served with great distinction and commitment at a senior level in both Democratic and Republican administrations. He is not a partisan. Rather, he has a well-earned reputation as a law enforcement professional and a skilled and even-handed prosecutor. Since leaving the government, Steve has established himself as one of the nation's top private practice lawyers and he serves as the managing partner of the Washington office of a leading international law firm.

Steve is not only an excellent lawyer, but he is also an experienced manager. As someone who currently oversees a large number of lawyers, I firmly believe that management experience is critical in a role such as the General

Counsel of the Department of Homeland Security. Steve has excelled at managing lawyers in both the government and in private practice.

Steve has everything that one could conceivably want for this critical position: deep expertise, the ability to manage, and, above all, impeccable character. I respectfully urge his speedy confirmation. Please do not hesitate to contact me if I can provide further information.

Sincerely yours,

Stuart A. Levey

TIMOTHY G. LYNCH
VICE PRESIDENT AND GENERAL COUNSEL

UNIVERSITY OF MICHIGAN

5010 FLEMING ADMINISTRATION BUILDING

September 11, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Re: Stevan E. Bunnell, Nominee for DHS General Counsel

Dear Chairman Carper and Ranking Member Coburn:

I write strictly in my individual, not institutional, capacity to recommend Steve Bunnell, who has been nominated to serve as the General Counsel of the Department of Homeland Security.

Steve Bunnell is a tremendously gifted lawyer who has impeccable judgment. I worked with Steve at the U.S. Attorney's Office and litigated an enforcement action against his client when he was in private practice. In those capacities I witnessed firsthand his first-rate judgment and analytical skills. Steve is truly a lawyer's lawyer and someone who believes in the rule of law.

Having served at the Department of Energy as the Acting General Counsel and Deputy General Counsel for Litigation and Enforcement, I have experience running a large federal agency's general counsel office. Based on that experience, I am fully confident that Steve Bunnell has the right temperament, experience, and skills to lead the DHS OGC. In particular, Steve has highly relevant experience in senior management positions at the Justice Department, including his tenure as the Chief of the Criminal Division for the U.S. Attorney's Office for the District of Columbia. Indeed, Steve's extraordinarily successful law enforcement career would serve him well advising senior leadership on legal issues arising at DHS.

Finally, Steve Bunnell is a man of great integrity, someone in whom you could have complete confidence that he would ensure that DHS and its leaders were serving the public interest in compliance with the letter and spirit of the law.

I appreciate your consideration and respectfully urge that Steve Bunnell be confirmed as the next General Counsel of the Department of Homeland Security.

Sincerely,

Timothy G. Lynch

Michael A. Mason
Chief Security Officer

verizon

One Verizon Way, VC54N121
Basking Ridge, NJ 07920

Phone 908 559-5628
michael.a.mason@verizon.com

August 30, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Carper and Ranking Member Coburn:

I am writing this letter in support of the nomination of Steve Bunnell to become the next General Counsel of the Department of Homeland Security. I retired from the Federal Bureau of Investigation in December, 2007. Prior to my retirement I served as an Executive Assistant Director responsible for the FBI's Criminal, Cyber, Response and Services Branch. Prior to this assignment I was the Assistant Director-in-Charge of the FBI's Washington Field Office and that is where I first became acquainted with Steve Bunnell.

I considered Steve one of the best partners we had in the United States Attorney's Office. As we worked to address very complex problems, Steve was steadily focused on working on identifying the most effective solution possible. Steve was not one who believed all intelligent thought began and ended at his desk. Rather, he understood all members of an investigative *team* can contribute to the sought after solution. More importantly, he allowed those voices to be heard and recognized. When I think back to times we shared discussing complex cases in a group setting, two of Steve's most important attributes come immediately to mind. Steve was a good listener and when he spoke, it was to everyone's benefit to listen closely to what he had to say. Steve struck me as being driven by logic and reason. He was able to contextually assess a situation and propose common sense solutions. His voice was one of reason and thoughtfulness.

Steve has an in-depth knowledge of a broad spectrum of federal law as a result of his tenure in the United States Attorney's Office in Washington. He has served as both a line-prosecutor and as the head of the office's Criminal Division. This fact gave him tremendous credibility with the agents and analysts from the FBI, with whom he worked on many complicated cases. His professional and executive experience will undoubtedly be immediately recognized as invaluable assets within DHS.

Steve is leaving a private sector job he enjoys because he genuinely believes he can add value to the work of DHS and because he is driven to serve his country. As a former senior executive with the FBI and a former U.S. Marine Corps captain, I have some sense of what makes one a solid leader. My bottom-line assessment of Steve Bunnell can be summed up as follows; when Steve led the charge, all willingly followed and when Steve was a teammate, all were happy to have him on board. He was fully engaged at all times.

Therefore, without any reservations, I highly recommend Steve Bunnell for the position of General Counsel for the Department of Homeland Security.

Sincerely,

Michael C. Mason

Office Of John C. Richter

1700 Pennsylvania Ave, NW
Suite 200
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737
www.kslaw.com

John C. Richter
Direct Dial: +1 202 626 5617
Direct Fax: +1 202 626 3737
jrichter@kslaw.com

September 10, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Re: Nomination of Stevan E. Bunnell to be the General Counsel of the Department of Homeland Security

Dear Chairman Carper and Ranking Member Coburn:

I write in support of the nomination of Steve Bunnell to be the next General Counsel of the Department of Homeland Security. I got to know Steve first during my tenure in the Department of Justice, where, among other positions, I served as the United States Attorney for the Western District of Oklahoma (2005-2009) and as Acting Assistant Attorney General in charge of the Criminal Division (2005). Since my time in government, I have interacted with him on various legal and professional matters.

Steve embodies all the best qualities and experience needed for this position and to serve the American people admirably. He is a man of the highest integrity, an exceptional legal talent, highly competent, pragmatic, and down to earth. He has strong managerial experience and, having served many a general counsel in private practice, a keen appreciation for what is needed to represent an institutional client, like the Department of Homeland Security. He is well respected among his peers in the government, law firms, and private industry. And, as long-time career prosecutor, he understands whom he will be serving during his tenure back in government – the American people.

I cannot recommend him more highly. We are very fortunate that a man of his ethics, judgment, and capability is willing to return to government for this service. If I can provide you or your respective staffs with further information, please do not hesitate to contact me.

Sincerely,

John C. Richter

JCR:das

McGuireWoods LLP
2001 K Street N.W.
Suite 400
Washington, DC 20006-1040
Phone: 202.857.1700
Fax: 202.857.1737
www.mcguirewoods.com

J. Patrick Rowan
Direct: 202.857.1758

prowan@mcguirewoods.com
Direct Fax: 202.828.3304

September 11, 2013

VIA E-MAIL AND FIRST CLASS MAIL

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Carper and Ranking Member Coburn:

I write to support the nomination of Stevan Bunnell to serve as the General Counsel of the Department of Homeland Security (DHS).

Steve and I worked together at the U.S. Attorney's Office for the District of Columbia (USAO) and thereafter when he served as Chief of the USAO's Criminal Division while I was working on national security matters in the Justice Department's Criminal Division and National Security Division. I have enormous respect for Steve's character and intellect and I am certain that, if confirmed, he will serve DHS with distinction in this challenging position.

Steve is well prepared to take on the job of General Counsel, a significant aspect of which will involve the supervision of a large number of lawyers and issues within the Office of General Counsel. He has successfully managed lawyers and other at the USAO and at O'Melveny & Myers for over ten years. Having worked for him briefly, I know that he is fair but firm in overseeing his staff, and I expect that his management will produce an exceptionally productive and professional environment within the Office of General Counsel.

Many of the issues that face the General Counsel relate to law enforcement matters. As a result of his many years of work as a line prosecutor and supervisor of prosecutors, Steve has a deep understanding of the legal issues that face law enforcement, including the need for legal guidance that is clear and easily applied in the field. Steve's experience includes work on terrorism issues and cases, so he is familiar with the unique set of pressures that comes with matters implicating our nation's security.

Moreover, Steve possesses outstanding professional judgment, honed by many years of work on complicated law enforcement matters, as well as significant experience in private practice. Early on in his career at the USAO, Steve distinguished himself by his ability to examine issues in a calm and reasoned manner and provide wise advice to colleagues. His exposure to challenging matters in several higher level positions since then has added considerably to his capacity for analyzing difficult questions. I am confident that he will be a valued legal advisor to the senior management of DHS and that his advice will be the same without regard to political considerations.

I applaud Steve's nomination and I commend him to you without reservation.

Sincerely,

J Patrick Rowan

Raytheon

Integrated Defense Systems
Office of the General Counsel
50 Apple Hill Drive
Tewksbury, Massachusetts
01876 USA
978 858-4216

September 12, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security
and Government Affairs
340 Dirksen Senate Office Building
Washington DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security
and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Re: Stevan E. Bunnell

Dear Chairman Carper and Ranking Member Coburn:

I write to convey my support for Steve Bunnell's nomination to serve as General Counsel of the Department of Homeland Security. Steve's experience, good sense, integrity, and capabilities make him supremely qualified for this important position.

Steve and I worked closely together during my tenure as United States Attorney for the District of Columbia from 2006 – 2009. Even prior to then, however, I knew of Steve by way of his stellar reputation in both the U.S. Department of Justice and the Washington, DC legal community. His lengthy DOJ service, including leadership positions in multiple administrations of differing political casts, speaks to his talent, fair-mindedness, and devotion to non-partisan, careful adherence to the law. His successful tenure as the Managing Partner of the Washington, DC office of a large international law firm demonstrates not only strong leadership skill, but also a facility with the private sector which will serve him well as the general counsel of an agency that needs to interact positively with that sector.

During my time with Steve in the U.S. Attorney's Office, he served as the Chief of the office's Criminal Division. In that role he managed our significant federal court practice (employing some 85 Asst. U.S. Attorneys and 45 support personnel), which investigates and prosecutes exceedingly complicated cases in areas such as public corruption, corporate fraud, securities fraud, healthcare fraud, export control, and international terrorism. The Chief position requires ample intelligence, of course, but equally important attributes are managerial competence, leadership ability, sound judgment, integrity, a strong work ethic, and the ability to build and maintain effective relationships with federal and local law enforcement agencies, the bench, and the defense bar.

In my daily interactions with Steve he displayed these attributes in abundance. For example, Steve's keen intellect made him a "must have" in any discussion about important, substantive legal issues, whether originating in the Criminal Division or anywhere else in the office. As for sound judgment, I still remember Steve's wise, constant counsel – "What is the right thing to do?" – whenever we confronted difficult investigative or prosecutorial decisions. To be sure, Steve was appropriately fierce on behalf of the public when justified by the facts and the law. At the same time, Steve well understood that, given the awesome power federal prosecutors wield

and the consequences that ensue, sometimes the just course is choosing not to deploy that power. This reputation for devotion to duty, fairness, and integrity underpin the high regard one finds for him among federal agents, the defense counsel community, and the bench.

Steve also displayed tremendous skill in managing and leading the Criminal Division. Appreciating that the office had limited resources and embracing his obligation to husband those resources on behalf of the public, Steve effectively implemented prosecutorial priorities that furthered DOJ "national" goals (e.g., counterterrorism and corporate fraud) while making certain also to address priority problems in the District (e.g., violent drug trafficking and local corruption). He proved adept at identifying and developing talented performers in his organization, both at the line level and among the section supervisors who assisted him. It is telling that many who worked under his leadership have gone on to high-ranking positions in the U.S. Attorney's Office and at the Department of Justice.

A final word on Steve's leadership ability. He has the intelligence, courage, poise, and empathy that are the raw materials of a natural leader. But Steve possesses two additional traits that in my judgment mark his leadership prowess as authentic. First, Steve will gladly get into the trench with his troops, they know that, and they are thrilled to have him there. Second, Steve has held a number of important positions during his time in public service, and based on my experience with him, his motivation has always been the mission at hand, the public he serves, the job well done. Unlike many, he focuses exclusively on carrying out, to the best of his ability, the responsibilities of the position he holds. He is not concerned with the one next on the ladder

The Administration has hit the bulls-eye in selecting Steve Bunnell for this important position. The public would be getting in Steve a consummate public servant in whom they can have complete confidence and trust. I am honored to join those who are supporting Steve in this process, and please do not hesitate to call on me if I can provide further information.

Sincerely,

Jeffrey A. Taylor
VP & General Counsel
Raytheon Integrated
Defense Systems

4311 Elm Street
Chevy Chase, MD 20815

10 September 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Carper and Ranking Member Coburn:

I write in support of Stevan E. Bunnell's nomination to serve as General Counsel for the Department of Homeland Security. Steve is an exceptional lawyer with a distinguished record in both public and private practice. He brings a combination of leadership, judgment, experience and personal humility that insure he will succeed in the job. The country would be well-served by his confirmation.

I have worked with Steve in a variety of settings for the last fifteen years, dating back to when he was an Assistant United States Attorney in the District of Columbia and I had the same position in the District of Maryland. Given the immediate adjacency of the two Districts, it was not unusual for investigations to overlap and for the two offices to be pursuing the same potential defendants for criminal conduct that involved each location. As a result, there was also a healthy rivalry between the two offices to bring cases. Steve and I were both in management positions and therefore were sometimes left to work out coordinated positions that best served the United States overall when the work of the offices intersected. Throughout those years, Steve was a pleasure to have as a colleague – he showed both a laudable loyalty to the AUSAs he supervised in Washington, D.C., but also a willingness to compromise or defer to a neighboring district when that was in the best overall interests of justice. He was always smart on the law and smarter still in finding practical solutions to problems.

In subsequent years, I served both as a United States Attorney and as Assistant Attorney General at the Justice Department headquarters. Steve was, without doubt, one of the most capable attorneys with whom I ever served at the Department. Steve was the kind of sound, unflappable lawyer you turned to when you had a difficult problem and needed a good "second opinion." In doing so, you knew you would get both practical insight and unbiased fair-mindedness. As a result, he had the respect of both the United States Attorney under whom he served and those career attorneys that he led. In sum, Steve

brings broad experience in legal management, a track record of achievement, and a strength of character to "call them as he sees them" that are essential attributes of an agency general counsel.

I strongly urge the Committee's speedy and favorable consideration of his nomination.

Respectfully,

Ronald J. Tenpas
Former Assistant Attorney General, Environment and Natural Resources Division, 2007-2009
Former United States Attorney, Southern District of Illinois, 2003-05

CADWALADER

Cadwalader, Wickersham & Taft LLP
700 Sixth Street, N.W., Washington, DC 20001
Tel +1 202 862 2200 Fax +1 202 862 2400
www.cadwalader.com

New York London Charlotte Washington
Houston Beijing Hong Kong Brussels

September 3, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security
and Government Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security
and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Re: Stevan E. Bunnell

Dear Chairman Carper and Ranking Member Coburn:

I submit this letter in support of Steve Bunnell's nomination to serve as General Counsel of the Department of Homeland Security (DHS). I believe that Steve is the ideal candidate for this important position.

I write this letter with the benefit of several perspectives on Steve and the job for which he has been nominated. First, my experience in a variety of government attorney positions – U.S. Attorney, Assistant U.S. Attorney, Assistant Attorney General, and FBI General Counsel – has given me an understanding of the qualities that make for success in such a position. Second, my close working relationship with DHS during my service in those positions, and particularly when I served as Homeland Security Advisor to President Bush, gave me an appreciation for the important role that DHS and its counsel play in the homeland security community and the inter-agency process. Finally – and most importantly – my over twenty years as Steve's close friend and colleague have given me an insight into the man and the stellar qualities and character he will bring to that job.

Steve is ideally suited for this job in a number of ways. First, he has a wealth of relevant experience that will allow him to hit the ground running. His many years as a career prosecutor and Justice Department official handling highly sensitive law enforcement and national security matters have provided him a very solid grounding in both the substance of the issues he will face and the government processes through which those issues are addressed.

Kenneth L. Wainstein Tel +1 202 862 2474 Fax +1 202 862 2400 ken.wainstein@cwt.com

The Honorable Thomas R. Carper
The Honorable Tom A. Coburn, M.D.
September 3, 2013

Steve is also a man with proven leadership skills – skills that are necessary for a General Counsel who is responsible for both managing an extended group of DHS lawyers across a wide spectrum of agencies as well as representing the Department with strength and credibility in the inter-agency process. Steve's leadership qualities have stood out throughout his career – from his service as Chief of the Criminal Division when we were together at the United States Attorney's Office to his successful tenure as Managing Partner of O'Melveny's D.C. office over the past few years. At every step of his career, Steve has proven himself a natural leader who sets the example for the rest of his colleagues.

Lastly, Steve is a man who has the integrity, the human decency and the strong moral compass one would want in such an important and sensitive position. Steve is universally respected and admired by all who have ever worked with him – from the Attorneys General and Deputy Attorneys General of both parties who have relied on his counsel to the O'Melveny associates who have flourished under his candid and inclusive management style. Steve has earned that admiration, in part by his smarts and hard work, but also by forging a reputation throughout his many years in government as the quintessential public servant – as a man who subordinates all personal or political interests and focuses exclusively on doing what is right for his agency's mission and for his country. His willingness to step out of a highly successful law firm partnership and into the DHS counsel position is just the most recent example of Steve's selflessness and sense of duty.

In sum, I cannot think of a more qualified or deserving candidate for this position. Please do not hesitate to call on me if I can provide further information. It is an honor to lend my voice to the many others from all parts of the political spectrum who admire and support Steve in this confirmation process.

Sincerely,

Kenneth L. Wainstein

September 16, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security & Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC, 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security & Governmental Affairs
442 Hart Senate Office Building
Washington, DC, 20510

Dear Chairman Carper and Ranking Member Coburn,

I am writing to you today to enthusiastically support the nomination of Ms. Suzanne E. Spaulding as the Under Secretary for the National Protection and Programs Directorate at the Department of Homeland Security.

I am sure you are already familiar with Ms. Spaulding's extensive experience and record of service. She has consistently demonstrated leadership and vision in both the public and private sectors; in state, federal and international domains; in fields ranging from the highest levels of the Intelligence community to the most senior levels of government; and in both legislative and executive branches while serving both Democratic and Republican Administrations.

In addition to holding a world-class resume, I would respectfully point the Committee's attention to how Ms. Spaulding's unique experience especially suites her for the position to which she has been nominated. The job of strengthening our nation's critical infrastructure from both physical and cyber threats demands the vast expanse of experience that Ms. Spaulding (and few others) possess.

The threats we face today are both domestic and international. The jurisdictions that must be activated and coordinated are wide ranging and most of the infrastructure itself is privately owned but alternatively subject to government's regulatory control or the free market. I believe only someone who knows and

2500 Wilson Boulevard Arlington, VA 22201-3834 United States of America (t) 703 : 907-7090 (f) 703 : 907-7093

understands how this multitude of variables works and interacts is capable of doing the sort of pressurized job that6 this Under Secretary post demands. I believe Ms. Spaulding is uniquely suited to this task.

Finally, I would like to speak briefly not just to Ms Spaulding's expertise, but, just as importantly, to her demeanor. Security in the digital world we now inhabit can no longer be thought of as simply a governmental function sometimes carried out by the private sector. Instead, a sustainable security system must grow from a true and sincere partnership.

While both industry and government face similar risks, their assessments of risk are aligned but not identical, as government and industry have legally determined differences in priority. Yet, we jointly have must find a way to construct a unified national security posture notwithstanding these inherent differences. To accomplish this elusive goal we need individuals who are open to new ideas and are willing to listen to the legitimate needs of their partners so that a mutually secure and sustainable system can be delivered.

In all candor we do not find that open and collaborative attitude universally. However, we do believe we find that approach to problem solving in Ms Spaulding's character and perhaps this above all makes me feel optimistic about her chances to succeed in all of our mutual self interest if she is successfully confirmed.

I would like to endorse Ms. Spaulding's candidacy without reservation and respectfully urge the Committee to support her nomination as well.

As always, I would be delighted to offer the Committee any other assistance they may require.

Sincerely,

Larry Clinton

Larry Clinton
President/CEO
Internet Security Alliance

2500 Wilson Boulevard Arlington, VA 22201-3834 United States of America (t) 703 / 907-7090 (f) 703 / 907-7093

Northeastern University
George J. Kostas Research Institute for Homeland Security

13 September 2013

Senator Thomas R. Carper
Chairman, Committee on Homeland Security and Governmental Affairs
U.S. Senate
Washington, DC 20510

Senator Tom Coburn
Ranking Member, Committee on Homeland Security and Governmental Affairs
U.S. Senate
Washington, DC 20510

Dear Chairman Carper and Ranking Member Coburn:

George J. Kostas Research Institute for Homeland Security
kostasinstitute@neu.edu
northeastern.edu/kostas
Burlington Campus
141 South Bedford St.
Burlington, MA 01803
781.238.8140
Main Campus
960 Renaissance Park
360 Huntington Ave.
Boston, MA 02115
617.373.6090

I am the Founding Co-director of the George J. Kostas Research Institute S. Homeland Security and Professor of Political Science at Northeastern University. Since before 9/11 when I served on the staff of the U.S. Commission on National Security in the 21st Century (Hart-Rudman Commission), I have devoted my professional life to informing and advancing the homeland security mission.

I am writing today to provide my most enthusiastic endorsement of Suzanne E. Spaulding to be the next DHS Under Secretary for National Protection and Programs. I have known Suzanne for more than a decade and over that time I have found her to an outstanding leader, a talented manager, and consummate professional with a razor-sharp mind and impeccable judgment. I deeply admire and respect her expertise on national security and homeland security matters. She is a true patriot who is unerring in her commitment to do all that can be done towards making our great nation safer. Finally, to paraphrase John Paul Jones, she is a woman who possesses "the finest sense of honor." You should confirm her without reservation.

Sincerely,

Stephen Flynn, Ph.D.
Professor and Founding Co-Director
George J. Kostas Research Institute for Homeland Security

September 12, 2013

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington DC 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
Committee on Homeland Security and
Governmental Affairs
United States Senate
442 Hart Senate Office Building
Washington DC 20510

Dear Mr. Chairman and Ranking Member Coburn:

I write in support of the nomination of Suzanne Spaulding to serve as Under Secretary of Homeland Security for the National Protection and Programs Directorate.

I am a former Republican Staff Director of the then-Governmental Affairs Committee for Ranking Member Fred Thompson. In that capacity, I was the lead Republican staff member handling the legislation that created the Department of Homeland Security in 2002 (and worked with Rick Kessler on that and other matters). Subsequently, as an appointee at the Department of Justice from 2003-07, there were a number of occasions during which I worked closely with DHS, including what is now its National Protection and Programs Directorate. Most recently, as Staff Director and Chief Counsel of the House Judiciary Committee, I again had a number of dealings with DHS. As a result, I know the agency reasonably well.

I also know Ms. Spaulding well. I served as chief counsel of the Judiciary Committee's Subcommittee on Terrorism, Technology and Government Information under Chairman Arlen Specter when he also served as Chairman of the Select Committee on Intelligence in 2005-07, during which time Ms. Spaulding served as SSCI's General Counsel. We worked closely together on a number of sensitive issues that crossed our jurisdictional lines, especially involving international terrorism.

Ms. Spaulding is an extremely well-qualified nominee. Her record speaks for itself and I will not amplify it. I will note the relevance of some of her experience. Her positions as a congressional aide in both the Senate and the House and for both Republicans and Democrats give her a deep appreciation of the role of Congress in policy development and oversight. Her positions at the Central Intelligence Agency and with several executive commissions provide a wealth of

relevant experience for the role for which she has been nominated. Her stint in the private sector gives her an appreciation for the important role and the interests of non-government entities that people in government may sometimes overlook. And her recent experience at DHS in the Directorate will allow her to hit the ground running as the confirmed head of the office.

DHS is not the place for on-the-job training, and Ms. Spaulding is one person who will not need any. The National Protection and Programs Directorate at DHS is also not a place for partisan politics, and here too Ms. Spaulding is uniquely qualified. It is today the very rare individual who has policy-development experience serving both political parties. Ms. Spaulding's service to both parties demonstrates her true qualification: she is the consummate national security professional.

In an era when finding the best people to serve our country gets harder and harder, we may consider ourselves fortunate that someone like Ms. Spaulding would forego the private sector for the long hours, the anonymity, and the tension that go along with protecting our national security while preserving our civil liberties. I am pleased to consider Ms. Spaulding a friend and am grateful she is willing to continue in public service. I encourage the Committee's prompt consideration and endorsement and the Senate's confirmation of her nomination.

I would be pleased to expand in any way on my endorsement of Ms. Spaulding and can be reached during business hours at 202-662-5669.

Respectfully,

Richard A. Hertling

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

September 10, 2013

The Honorable Tom Carper
Chairman
Senate Committee on Homeland Security and
Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Carper:

I write in support of the nomination of Suzanne Spaulding to be Under Secretary at the U.S. Department of Homeland Security.

Ms. Spaulding currently serves as the Deputy Under Secretary for the National Protection and Programs Directorate at the Department of Homeland Security, overseeing Infrastructure Protection, US-VISIT, and the Federal Protective Service – initiatives that mitigate risk to our critical infrastructure, including Federal facilities.

Ms. Spaulding also served as the Executive Director of both the National Commission on Terrorism and the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction. She worked on critical infrastructure sectors, such as nuclear power, after the terrorist attacks on September 11, 2001. Her well-established expertise in areas including intelligence, terrorism, critical infrastructure protection, biodefense and nuclear weapons has undoubtedly contributed to our national security.

With over two decades of experience working on national security issues, Ms. Spaulding has proven her dedication to serving and strengthening this Nation, working for both Republican and Democratic Presidential Administrations and elected officials in Congress and state government. She is an excellent nominee for this position, and I hope that the Senate Committee on Homeland Security and Governmental Affairs will move quickly to report her nomination to the Senate.

Sincerely,

PATRICK LEAHY
Chairman

12 September 2013

Senator Tom Carper
Chairman
Senate Homeland Security and Governmental Affairs Committee
United States Senate
Washington, D.C.

Dear Senator:

I would like to write in support of the nomination of Suzanne Spaulding to serve as Under Secretary for the Department of Homeland Security's National Protection and Programs Directorate.

I have known Suzanne for many years. She is without a doubt one of the most capable individuals in Washington with deep expertise and a strong background in policy making and law that makes her an ideal candidate for this position. Suzanne's experience spans both public and private sectors. She has unparalleled governmental experience, having worked in both the House and the Senate and in the Executive Branch, for both Republican and Democratic Administrations.

Suzanne has a remarkable knowledge of security and intelligence issues that would serve her well as Under Secretary. She also has a clear understanding of the role of the private sector in homeland security and infrastructure protection and of the importance of partnerships to strengthen critical infrastructure protection. Suzanne was one of the members of the CSIS Commission on Cybersecurity for the 44th Presidency and made invaluable contributions to our work. She is one of the people I regard as an expert on cybersecurity here in the Washington. She is a strong defender of the need to protect privacy and civil liberties and to take them into account when designing or implementing policy.

An equally important attribute is Suzanne's ability to think strategically about the problems of critical infrastructure protection, cybersecurity and the mission of the Department. She has thought deeply about these issues and would make a significant contribution to both the Department and our nation's security. I respectfully ask that you and the other member of the Committee consider favorably her nomination.

Sincerely,

J. A. Lewis

James Andrew Lewis
Center for Strategic and International Studies
Washington, D.C.

Center for National Security Studies
protecting civil liberties and human rights

Director
Kate Martin

September 17, 2013

The Honorable Thomas Carper, Chair
The Honorable Tom Coburn, Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, D.C.

Re: Nomination of Ms. Suzanne E. Spaulding

Dear Senators Carper and Coburn:

I write to strongly support the nomination of Ms. Suzanne Spaulding to be Undersecretary for National Protection and Programs Directorate at The Department of Homeland Security.

I have worked on issues at the intersection of civil liberties/human rights and national security for almost twenty-five years and have known Ms. Spaulding for many years. I have had the pleasure of working with her on some specific projects and the benefit of her wise and thoughtful views on many issues. I have closely read her writings and carefully listened to many of her speeches. She is always extremely thoughtful, knowledgeable and wise about the difficult national security questions faced by the government in protecting the American people. I know that Ms. Spaulding is genuinely respectful of the views of others, truly interested in understanding all aspects of a problem and superbly competent at achieving consensus and solutions that address differing interests. She is a model public servant devoted to the national interest and committed to protecting both the national security of the United States and our constitutional rights and liberties. She has a deep understanding and respect for privacy, free expression, transparency and accountability in government and has worked to protect the national security consistently with respect for our constitutional rights and democratic government. I would be happy to provide any further information that you might find useful.

Thank you for consideration of my views.

Sincerely,

Kate Martin

Kate Martin
Director, Center for National Security Studies
(affiliation listed for identification purposes only).

1730 Pennsylvania Ave NW, 7th Floor, Washington, D.C. 20006
tel: (202) 721-5650 fax: (202) 530-0128 kmartin@cnss.org

The Honorable Tom Carper
United States Senate
513 Hart Senate Office Building
Washington, DC 20510

September 12, 2013

RE: Letter of Recommendation for Suzanne Spaulding as Under Secretary for the National Protection and Programs Directorate, DHS

Dear Chairman Carper,

I am writing to urge your serious consideration of Ms. Suzanne Spaulding to the position of Under Secretary for the National Protection and Programs Directorate (NPPD) within the Department of Homeland Security. Ms. Spaulding brings a recognized career of skilled, non-partisan leadership and expertise on national security issues, including homeland security, intelligence, terrorism, critical infrastructure protection, cybersecurity, law enforcement, foreign investment, biodefense, crisis management, and threats posed by weapons of mass destruction.

As both the Defense Information Systems Agency Director and the Manager of the National Communications System during a period that included the 9/11 terrorist attacks, I recognize the importance of having experienced, competent leaders in providing critical national security and emergency preparedness capabilities – across government and industry – in supporting our National leaders. I believe that I have a good understanding of what the NPPD responsibility entails and the expertise required. Through my experience in working with Ms. Spaulding, I can attest that she possesses the skills, experience, and leadership to continue making positive, lasting differences across the Department and our Nation. Most recently, I served as Co-chair of the CSIS Commission on Cybersecurity for the 44th Presidency where Ms. Spaulding was a member and key contributor in producing three reports that were well-respected by the President, members of Congress, and other key government and industry leaders.

Ms. Spaulding has a record of outstanding accomplishments and leadership serving in both government and industry, including the U.S Senate, U.S. House of Representatives, the Central Intelligence Agency, and in a leading consulting firm. She is accomplished in working national security issues for both Republican and Democratic Administrations and on both aisles of Congress. Ms. Spaulding's strongest qualifications, however, are leadership and team building. She has consistently built, led, and nurtured teams that have achieved innovative, significant results. I highly recommend Ms. Spaulding for this position and for increased responsibility within the Department of Homeland Security.

Very respectfully,

Harry D. Raduege, Jr., Lieutenant General, USAF (Ret)
Former Director, Defense Information Systems Agency and Manager, National Communications System

September 12, 2013

The Honorable Tom Carper
Chairman
Senate Homeland Security and Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC, 20510

The Honorable Tom Coburn
Ranking Member
Senate Homeland Security and Governmental Affairs Committee
442 Hart Senate Office Building
Washington, DC, 20510

Dear Chairman Carper and Ranking Member Coburn,

I am writing to express my support for the nomination of Suzanne E. Spaulding to be Under Secretary for National Protection and Programs at the Department of Homeland Security (DHS).

Ms. Spaulding is a brilliant and talented leader whose commitment to national and homeland security has been demonstrated throughout her career in both the government and the private sector. Her deep understanding of counterterrorism, infrastructure protection and cybersecurity will serve DHS and the nation well.

I knew of Ms. Spaulding's keen mind and security policy expertise long before I became acquainted with her personally. In 2008, I had the chance to work with Suzanne directly when we both served on the CSIS Commission on Cybersecurity for the 44th Presidency. I came to know Suzanne as a strategic thinker with a firm grasp of homeland security legal and policy issues and an acute understanding of the workings of government. Suzanne's leadership skills were also evident. Ms. Spaulding provides a calm, rational voice that charts the path to common ground.

As a former Deputy Under Secretary of the National Protections and Programs Directorate (NPPD), I am familiar with the skills needed to lead this organization. One must be strategic but focused on details when required, directed toward operational goals, respected by stakeholders both private and public, and possess strong management skills. I am confident that Suzanne Spaulding embodies all of these traits.

It is without hesitation that I recommend the confirmation of Suzanne Spaulding. She is a valuable asset to DHS, and is the perfect choice to carry forward Rand Beers' leadership of NPPD.

Sincerely,

Philip Reitinger

September 5, 2013

The Honorable Thomas R. Carper
Chairman
Senate Homeland Security and Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Thomas A. Coburn
Ranking Member
Senate Homeland Security and Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Carper and Ranking Member Coburn:

We are writing in strong support of the nomination of Suzanne Spaulding to be an Under Secretary at the Department of Homeland Security (DHS), leading the National Protection and Programs Directorate (NPPD). Ms. Spaulding is an excellent choice to lead NPPD and be in charge of the Department's critical missions of cybersecurity and infrastructure protection.

Ms. Spaulding has the right qualifications to lead NPPD, including her previous work at the Central Intelligence Agency, as a senior Congressional staffer on both the Senate and House intelligence committees, as a leader of the Standing Committee on Law and Security of the American Bar Association, and in the private sector. She has played an active role in the policy community for the last two decades, including serving as Executive Director of both the Deutch and Bremer Commissions, each of which played an important role in shaping homeland security and counterterrorism policy prior to the attacks of September 11, 2001.

She has served ably as a Deputy Under Secretary at NPPD for the last two years, including with respect to the implementation at DHS of Executive Order 13636 on cybersecurity and Presidential Policy Directive 21 on critical infrastructure.

As former homeland security officials in the George W. Bush Administration, we are confident that Ms. Spaulding would serve in a nonpartisan manner, focusing on implementing relevant laws and policies and maturing NPPD so that it can play the role that it must play within the federal government on cybersecurity and infrastructure protection issues.

Given Ms. Spaulding's strong qualifications, and also in light of the growing number of vacancies in other parts of DHS, we urge the Committee to move swiftly to consider her nomination.

Sincerely,

The Honorable Tom Ridge
Former Secretary of Homeland Security

The Honorable Michael Chertoff
Former Secretary of Homeland Security

The Honorable Stewart Baker
Former Assistant Secretary for Policy, DHS

Frank Cilluffo
Former Special Assistant to the President,
White House Office of Homeland Security

THE CONSTITUTION PROJECT

Safeguarding Liberty, Justice & the Rule of Law

September 11, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security & Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC, 20510

The Honorable Tom A. Coburn, M.D.
Ranking Member
U.S. Senate Committee on Homeland Security & Governmental Affairs
442 Hart Senate Office Building
Washington, DC, 20510

Dear Chairman Carper and Ranking Member Coburn:

I am writing to enthusiastically endorse the nomination of Suzanne Spaulding for Under Secretary for the National Protection and Programs Directorate at the Department of Homeland Security. I have known and worked with Ms. Spaulding for many years, and can think of no one who is more honest, capable, and intelligent than she is. She has enormous breadth and depth of experience and expertise on the issues relevant to the position for which she has been nominated.

Moreover, as someone who heads The Constitution Project, which seeks bipartisan consensus on constitutional issues, I understand fully how important Ms. Spaulding's service on both sides of the aisle is to achieving lasting, effective, and sensible results. This kind of service is becoming increasingly rare in Washington, and thus makes Ms. Spaulding's career and her past and future contributions even more vital to our country's health. Ms. Spaulding's work with the Constitution Project helped us to attain bipartisan consensus on a number of constitutional issues related to national security and the rule of law. It was a difficult balancing act, but Ms. Spaulding's skills at consensus-building and her deep knowledge of the issues were instrumental in our success.

I would be pleased to provide additional information. I hope you will approve Ms. Spaulding's nomination expeditiously. The country needs public servants like her.

Very truly yours,

Virginia E. Sloan

The Honorable Juan C. Zarate
5268 Winter View Drive
Alexandria, VA 22312
(703) 725-4156
jczarate@post.harvard.edu

September 17, 2013

The Honorable Thomas R. Carper
Chairman
U.S. Senate Committee on Homeland Security & Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC, 20510

RE: **Support for the Nomination of Suzanne E. Spaulding**

Dear Chairman Carper:

I am writing to endorse and support enthusiastically the nomination of Suzanne E. Spaulding to serve as Under Secretary for National Protection and Programs Directorate at the Department of Homeland Security (DHS).

Suzanne is a true homeland and national security expert and leader of the highest order. Suzanne will bring serious intellect and decades of relevant experience – including bipartisan sensibilities – to her work and this position. This nomination is an inspired choice that will ensure that the U.S. government has a highly qualified leader to manage some of the most difficult challenges tied to cybersecurity, infrastructure protection, biometric identity management, and national resilience.

I have been fortunate to work with and know Suzanne since I left the Bush Administration in January 2009, serving last as the Deputy Assistant to the President and Deputy National Security Advisor for Combating Terrorism. Suzanne and I have worked together to advise the Center for Strategic and International Studies, Transnational Threats Project, and also served as Senior Fellows to the George Washington University Homeland Security Policy Institute. In our work focusing on the future of terrorism threats, innovations in the homeland security domain, and the need for national resilience, Suzanne always distinguished herself with the depth and breadth of her experience, her keen perceptions, and sharp judgment.

Her background and experience speak for themselves and prepare her well to assume this role for DHS. Suzanne's distinguished career and significant experience in a range of disciplines in significant positions – from her work at the CIA to her role as general counsel to the Senate Select Committee on Intelligence – provide her with unique skills as a critical time for our nation's security. Importantly, she has reviewed, managed, and

dealt with some of the nation's most serious threats and deficits – and brings these critical insights and her background to address the myriad systemic vulnerabilities in our national infrastructure. As DHS grapples with some of the most difficult policy and legal questions, it needs Suzanne as part of its leadership team.

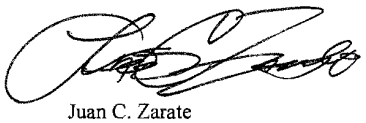
In whatever setting, Suzanne's leadership and voice are noticed and respected. Suzanne has always demonstrated an ability to lead through the strength of her ideas and a willingness to listen to the views and insights of others. Her work and history demonstrate that she has always been about results. With a warm personality and willingness to work with all stakeholders, Suzanne is well suited to lead her team and an organization like DHS.

I know Suzanne has already contributed significantly to the work of the Department. If confirmed, she will no doubt serve as one of the government's most important homeland security leaders. She will use that role wisely and well for the safety of our country and its interests.

I recommend fully that the Committee and Senate support Suzanne's nomination, for the sake of DHS and our country. She will serve us all well.

I am available to answer any questions or provide any further insights. Thank you for your time and consideration.

Sincerely,



Juan C. Zarate

○