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 protect the Nation's critical physical 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 infrastructure 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)

This 11th day of September, 2013

RANDOLPH SCOTT NOTARY PUBLIC DISTRICT OF COLUMBIA

District of Columbia: SS
Subscribed and Sworn to before me
this 11th day of September 2013

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 Director 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.