Response to Written Questions Submitted by Hon. John Thune to Hon. John Roth

Question 1. In your testimony, you also highlighted the consistently disconcerting results of penetration testing efforts, which identified vulnerabilities in TSA's Advanced Imaging Technology equipment. You observed, however, that in the last 18 months, TSA's response to the findings has exhibited "marked change from previous practice." What steps is TSA taking to mitigate the security vulnerabilities discovered in previous rounds of covert testing?

Answer. In response to our findings, TSA:

- Immediately created Tiger Teams with a 10-Point Plan to take action and correct the vulnerabilities identified in the 2015 tests. TSA's final Tiger Team report included root cause analyses, recommendations, action plans, and mitigation strategies;
- Worked with DHS' Tiger Team to develop a root cause analyses of checkpoint screening systems and human performance to explain why prohibited items were entering the sterilized area of federalized airports;
- Promptly briefed all Federal Security Directors of our 2015 test results;
- Conducted "Back to Basics" Mission Essentials/Threat Mitigation training for every Transportation Security Officer;
- Developed additional training to address: (1) the findings of the OIG's 2015 covert testing; (2) information gleaned from TSA's own covert testing; (3) relevant and current threat information, and (4) other areas identified by the Tiger Team;
- Addressed weaknesses in its standard operating procedures; and
- Is researching other technologies while trying to improve the capabilities of the existing equipment.

Question 2. At the hearing, you mentioned the importance of strengthening the cybersecurity of government information and systems. What are the most important steps the Secretary should take to increase the effectiveness of the agency's cybersecurity programs?

Answer. Our Fiscal Year (FY) 2016 FISMA evaluation of DHS' agency-wide security program indicates that DHS still has much to do to ensure the effectiveness of its cybersecurity programs.[1]

The Department can strengthen its oversight of its information security program for its unclassified, "Secret," and "Top Secret" programs at the component level. For example, DHS Components were not consistently following DHS' policies and procedures to:

(1) Keep system authorities to operate (ATO) current. As of June 2016, DHS had 79

[1] *Evaluation of DHS' Information Security Program for Fiscal Year 2016*, OIG-17-24 (January 2017).

unclassified systems operating under expired ATOs;[2]

(2) Consolidate all internet traffic behind the Department's trusted internet connections. As of August 2016, the Federal Emergency Management Agency (FEMA), Headquarters, Transportation Security Administration (TSA), and U.S. Secret Service (USSS) had not consolidated multiple connections behind trusted internet connections;

(3) Discontinue the use of unsupported operating systems that may expose DHS data to unnecessary risks;

(4) Implement all the required United States Government Configuration Baseline and DHS Baseline Configuration Settings, which, when fully implemented, help secure the confidentiality, integrity, and availability of DHS' information and systems;

(5) Mitigate security vulnerabilities by applying security patches timely; and

(6) Implement technology to prevent the activation of malicious links or attachments in phishing emails. As of September 2016, DHS and its Components had implemented only about 25 percent of the technology capability; FEMA and TSA had not begun their deployment efforts.[3]

Without addressing these deficiencies, the Department cannot ensure that its systems are adequately secured to protect the sensitive information stored and processed in them.

The Department is also responsible for providing crisis management, incident response, and defense against cyber-attacks for Federal.gov networks. However, as the Government Accountability Office (GAO) reported in January 2016, only 5 of 23 agencies were receiving intrusion prevention services.[4] Further, agencies had not taken all the technical steps needed to implement the Department's National Cybersecurity Protection System (NCPS), such as ensuring that all network traffic is routed through EINSTEIN sensors. GAO described the NCPS as limited in its effectiveness because it only detects known patterns of malicious data, but does not address threats that exploit many common security vulnerabilities. Moreover, it only monitors and blocks threats arriving by email, but does not address the common threats that web traffic may pose.

Through various audits, we also identified inadequate protection of DHS Components' sensitive systems and the data they contain. For example, due to inadequate controls, USSS employees were able to gain unauthorized access to the Component's Master Central Index system

---

[2] Under Secretary for Management Memorandum, *Strengthening DHS Cyber Defenses* (July 22, 2015).

[3] DHS requires that Components achieve Full Operational Capability within 90 days of the issuance of the Under Secretary for Management's January 13, 2016 memorandum. *See* Under Secretary for Management Memorandum, *Continuous Improvement of Department of Homeland Security Cyber Defenses* (January 13, 2016).

[4] *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (January 2016).

containing Representative Chaffetz's personally identifiable information.[5] DHS could better address insider threats by protecting against unauthorized removal of sensitive information via portable media devices and email, establishing processes for routine wireless vulnerability and security scans, and strengthening physical security controls to protect IT assets from possible theft, destruction, or malicious actions.[6] Moreover, the Department could develop a strategic implementation plan, a training program, and an automated information sharing tool to enhance coordination among its Components with cyber-related responsibilities.[7]

Question 3. As your respective offices issue recommendations based on audit and investigation work, what steps do you take to ensure that the recommendations are discrete tasks that are feasible for the agency to implement in a reasonable timeframe?

Answer. We make a concerted effort to ensure that our recommendations are concrete, reasonable, and practicable. In addition to drawing on our teams' extensive knowledge of Department and Component organization, programs, and operations, we work closely with the Department and Components throughout our reviews to ensure our recommendations are both feasible and effective. For example, we may:

- Conduct briefings with program officials to inform them of potential findings during the review so that they may begin to work on solutions or take corrective actions immediately;

- Provide program officials with formal notices of potential findings and recommendations during the audit and invite them to comment on our proposed recommendations. We then work with the agency to ensure the recommendations are feasible and address the underlying cause of the problem;

- Issue a draft report to the agency and, if warranted based on the agency's response, revise our recommendations before the final report is issued to the public; and

- Revise or administratively close a recommendation that is no longer relevant or feasible due to changing circumstances.

---

[5] *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*, OIG-17-01 (October 2016).

[6] *United States Coast Guard Has Taken Steps to Address Insider Threats, but Challenges Remain*, OIG-15-55 (March 2015); *Domestic Nuclear Detection Office Has Taken Steps To Address Insider Threat, but Challenges Remain*, OIG-14-113 (July 2014).

[7] *DHS Can Strengthen Its Cyber Mission Coordination Efforts*, OIG-15-140 (September 2015).

Response to Written Question Submitted by Hon. Deb Fischer to Hon. John Roth

Question. Inspector General Roth, in your written testimony, you expressed serious concern about the lack of a risk-based security strategy at TSA, particularly as it relates to surface transportation security and oversight. As you are aware, I have been working with leaders of this Committee to address these challenges at TSA. How has the TSA responded to your concerns since the September 2016 report was released? Has TSA made any progress in strengthening surface transportation security programs?

Answer. In November 2016, TSA provided us with an update on the actions it has taken to address the recommendations in our report, "TSA Needs a Crosscutting Risk-Based Security Strategy," OIG-16-134. TSA indicated that it expects to complete a risk-based security strategy that encompasses all transportation modes in the fourth quarter of FY 2017. TSA is also taking steps to integrate enterprise risk management with resource planning and expects to complete this process by December 31, 2020. Additionally, TSA has made some progress in implementing the three outstanding passenger rail transportation regulations required by the Implementing Recommendations of the 9/11 Commission Act of 2007. On December 16, 2016, TSA published two rulemakings in the Federal Register:

- Notice of Proposed Rulemaking for Security Training for Surface Transportation Employees, and

- Advance Notice of Proposed Rulemaking for Surface Transportation Vulnerability Assessments and Security Plans.

In January 2017, TSA reported it anticipates a Notice of Proposed Rulemaking for surface security vetting by the end of FY 2017. We anticipate an update from TSA in late April and will continue to monitor TSA's progress on addressing our recommendations.

Response to Written Question Submitted by Hon. Dean Heller to Hon. John Roth

Question. A difficulty for Inspectors General across federal agencies has always been getting the information they need and pushing back on the agency when they dispute the IG's claims.

It's something I've seen frequently at the Department of Veterans Affairs, and I've always felt very strongly that IG's must be willing to confront agencies to get the information they need to conduct a full investigation.

Have any of you had difficult accessing the information you need to hold your agency accountable and are there tools you need from Congress to increase transparency?

Answer. As I testified at the hearing, historically, we have not had difficulty accessing the information we need to hold the Department accountable. However, after the hearing, I was made aware of an internal procedure at TSA restricting and delaying our access to documents. Specifically, I learned that on October 3, 2016, "TSA HQ - Executive Advisor" sent a communication to TSA's "Office of Security Capabilities Federal" setting out instructions for interacting with the OIG. Among other things, the email notifies TSA personnel that documents responsive to an OIG request must first be "cleared" within TSA before being provided to the OIG. The email also states that, prior to production to the OIG, documents are to be subjected to multiple levels of review within TSA, including review by a Designated Program Office, OSC Audit Liaison Team, Office of Chief Counsel (OCC), and TSA leadership. Further, in a March 14, 2016 email attached to the October 2016 email, TSA personnel were instructed to inform TSA senior leadership of all interviews with, and productions of documents to, the OIG.

These TSA requirements are contrary to previous DHS practice, violate the letter and intent of the Inspector General Act of 1978 as amended and DHS directives, and chill confidential communication with the OIG. While the October 2016 communication is addressed to a specific subset of TSA employees, we are concerned that it may reflect unwritten practices followed by other TSA offices and employees, or that other TSA offices might use this communication as guidance for responding to OIG requests. We are attempting to determine the scope of the issue within TSA, and address this with TSA senior leadership. If we fail to resolve this issue to our satisfaction, we will issue a public report with our findings.