A LOOK AHEAD: INSPECTOR GENERAL RECOMMENDATIONS FOR IMPROVING FEDERAL AGENCIES

HEARING BEFORE THE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE ONE HUNDRED FIFTEENTH CONGRESS FIRST SESSION FEBRUARY 8, 2017
Printed for the use of the Committee on Commerce, Science, and Transportation
CONTENTS

Hearing held on February 8, 2017 ................................................................. 1
Statement of Senator Thune ........................................................................... 1
Statement of Senator Nelson ......................................................................... 3
Letter dated February 6, 2017 to Hon. Bill Nelson from Mary Mitchelson, Inspector General, Corporation for Public Broadcasting ................................................................. 9
Letter dated February 6, 2017 to Hon. Bill Nelson from Jon Hatfield, Inspector General, Federal Maritime Commission ................................................................. 16
Letter dated February 7, 2017 to Hon. Bill Nelson from Tom Howard, Inspector General, Amtrak ................................................................. 21
Letter dated February 7, 2017 to Hon. Bill Nelson from Allison C. Lerner, Inspector General, National Science Foundation ................................................................. 34
Statement of Senator Blumenthal ................................................................... 101
Statement of Senator Wicker ........................................................................ 103
Statement of Senator Blunt ........................................................................... 104
Statement of Senator Klobuchar ...................................................................... 106
Statement of Senator Cantwell ........................................................................ 108
Statement of Senator Inhofe ........................................................................... 110
Statement of Senator Booker ......................................................................... 111
Statement of Senator Cortez Masto ................................................................. 113
Statement of Senator Capito .......................................................................... 115
Statement of Senator Cruz ............................................................................ 117
Statement of Senator Duckworth ................................................................... 119

WITNESSES

Allison C. Lerner, Inspector General, National Science Foundation ............. 39
Prepared statement ........................................................................................ 41
Hon. Peggy E. Gustafson, Inspector General, U.S. Department of Commerce .. 45
Prepared statement ........................................................................................ 47
Prepared statement ........................................................................................ 57
Hon. Calvin L. Scovel III, Inspector General, U.S. Department of Transportation ................................................................. 86
Prepared statement ........................................................................................ 87

APPENDIX

Response to written questions submitted to Allison C. Lerner by:
Hon. John Thune ......................................................................................... 127
Hon. Deb Fischer ......................................................................................... 128
IV

Response to written questions submitted to Allison C. Lerner by—Continued

<table>
<thead>
<tr>
<th>Questioner</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hon. Dean Heller</td>
<td>128</td>
</tr>
<tr>
<td>Hon. Bill Nelson</td>
<td>128</td>
</tr>
<tr>
<td>Response to written questions submitted to Hon. Peggy E. Gustafson by:</td>
<td></td>
</tr>
<tr>
<td>Hon. John Thune</td>
<td>130</td>
</tr>
<tr>
<td>Hon. Deb Fischer</td>
<td>131</td>
</tr>
<tr>
<td>Hon. Dean Heller</td>
<td>132</td>
</tr>
<tr>
<td>Hon. Bill Nelson</td>
<td>132</td>
</tr>
<tr>
<td>Hon. Cory Booker</td>
<td>133</td>
</tr>
<tr>
<td>Hon. Tom Udall</td>
<td>133</td>
</tr>
<tr>
<td>Response to written questions submitted to Hon. John Roth by:</td>
<td></td>
</tr>
<tr>
<td>Hon. John Thune</td>
<td>135</td>
</tr>
<tr>
<td>Hon. Deb Fischer</td>
<td>136</td>
</tr>
<tr>
<td>Hon. Dean Heller</td>
<td>137</td>
</tr>
<tr>
<td>Hon. Bill Nelson</td>
<td>138</td>
</tr>
<tr>
<td>Hon. Cory Booker</td>
<td>138</td>
</tr>
<tr>
<td>Hon. Tom Udall</td>
<td>140</td>
</tr>
<tr>
<td>Response to written questions submitted to Hon. Calvin L. Scovel III by:</td>
<td></td>
</tr>
<tr>
<td>Hon. John Thune</td>
<td>142</td>
</tr>
<tr>
<td>Hon. Roy Blunt</td>
<td>144</td>
</tr>
<tr>
<td>Hon. Deb Fischer</td>
<td>144</td>
</tr>
<tr>
<td>Hon. Dean Heller</td>
<td>145</td>
</tr>
<tr>
<td>Hon. Todd Young</td>
<td>146</td>
</tr>
<tr>
<td>Hon. Bill Nelson</td>
<td>147</td>
</tr>
<tr>
<td>Hon. Tom Udall</td>
<td>148</td>
</tr>
</tbody>
</table>
A LOOK AHEAD:
INSPECTOR GENERAL RECOMMENDATIONS
FOR IMPROVING FEDERAL AGENCIES

WEDNESDAY, FEBRUARY 8, 2017

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m. in room SD–G50, Dirksen Senate Office Building, Hon. John Thune, Chairman of the Committee, presiding.

Present: Senators Thune [presiding], Wicker, Blunt, Cruz, Fischer, Heller, Inhofe, Johnson, Capito, Gardner, Young, Nelson, Cantwell, Klobuchar, Blumenthal, Booker, Udall, Peters, Duckworth, Hassan, and Cortez Masto.

OPENING STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

The CHAIRMAN. Good morning. This hearing will come to order.

Last week, this Committee held a hearing on reducing unnecessary regulatory burdens. We heard from stakeholders representing several sectors of the American economy about ways government agencies can regulate smarter, protecting public safety and market fairness while fostering economic growth and innovation.

Today, we will discuss another important way to make government more efficient and effective, by identifying and eliminating waste, fraud, and abuse in Federal departments and agencies. For this task, there is no more effective tool than the Inspectors General.

Created by the Inspector General Act of 1978, IGs serve as watchdogs over more than 70 Federal agencies. According to the Council of Inspectors General on Integrity and Efficiency, agency incorporation of IG recommendations led to $26 billion in potential savings in Fiscal Year 2015, and IG criminal and civil cases led to another $10.3 billion returned to the treasury. These figures amount to $14 saved for every taxpayer dollar invested in the work of the IGs.

This year marks the beginning of a new administration, and it will be important for new department and agency heads to be fully aware of the issues that have plagued their organizations in recent years. Each of the IGs on the panel today recently published the top management challenges of their agencies for the new fiscal year. In addition to these, we will be discussing some of the hun-
dreds of IG recommendations that remain open after, in some cases, several years.

The Department of Commerce faces a number of challenges across its agencies. For example, the National Oceanic and Atmospheric Administration manages the acquisition and development of critical weather satellites and will have to address cost and schedule overruns while avoiding gaps in satellite coverage.

FirstNet, which is an independent authority within the Commerce Department, is also reaching critical early stages in its rollout of a nationwide public safety broadband network, and I believe FirstNet will continue to benefit greatly from rigorous oversight by the Inspector General.

New Commerce Department leadership will also have to ensure that all of the Department’s employees respect and follow government spending rules in the wake of an IG investigation into unjustified spending by the former Under Secretary for International Trade. The National Science Foundation will have to address significant issues it has had keeping its large facilities, such as the National Ecological Observatory Network, or NEON, on time and on budget. The Committee ensured additional oversight of these facilities in the American Innovation and Competitiveness Act, and we’ll be eager to see these implemented.

The Department of Homeland Security oversees two components that are essential for ensuring the safety of our nation’s transportation system, the U.S. Coast Guard and the Transportation Security Administration. The Coast Guard will have to tackle the challenges of improving cybersecurity, information management, and financial reporting.

TSA has had several high profile issues in recent years, including airport security failures discovered by IG red team testing, as well as breaches involving the Secure Identification Display Area, or SIDA, badges of airport employees. The Committee worked to address these issues in the FAA Extension, Safety, and Security Act of 2016, but new department leadership will have to continue to work with DHS OIG to ensure the ongoing safety of the traveling public.

Finally, the Department of Transportation’s major challenges include setting up the playing field for revolutionary new transportation technologies such as unmanned aerial vehicles and self-driving vehicles while also maintaining a world class standard of safety. The Department must also more effectively manage the series of major upgrade programs to the National Airspace System known collectively as NextGen and ensure the effective implementation of the provisions of the FAST Act. This work will inform our discussions as we work to craft an FAA reauthorization bill this year.

Finally, I would like to address briefly some recent developments within the IG community. The media has reported that the new administration’s transition team considered removing some IGs. It appears, however, that they quickly changed their minds and notified these IGs, including Mr. Roth and Mr. Scovel, that they would not be removed. I am confident that incoming agency leadership will continue to find the oversight work of their IGs to be as invaluable as I have.
We have testifying before us today a distinguished all-IG panel. The Honorable Peggy Gustafson, Inspector General of the Department of Commerce, who, I would note, has been on the job at Commerce for only about 3 weeks although she is a veteran IG; Ms. Allison Lerner, Inspector General of the National Science Foundation, who also has served for nearly 20 years in leadership roles within the Commerce Department IG’s office; the Honorable John Roth, Inspector General of the Department of Homeland Security, who spent 25 years in high-profile positions within the Department of Justice; and the Honorable Calvin Scovel III, Inspector General of the Department of Transportation, who last year celebrated a decade of service as DOT’s Inspector General, which followed a distinguished 29-year career with the U.S. Marine Corps.

I want to thank you all for being here and look forward to a productive discussion.

I will now turn to Ranking Member Nelson for any opening remarks that he would like to make.

STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator NELSON. Thank you, Mr. Chairman.

Inspectors general throughout the Federal Government play a critical role in ferreting out waste, fraud, and abuse and ensuring that agencies serve as good stewards of taxpayer dollars. So thank you for what you do.

I’ll give you an example. The Department of Commerce IG’s office identified $1 billion in financial benefits and potential cost savings for four fiscal years while receiving $225 million in appropriations. That’s a return on investment of more than $5 for every single dollar invested in that office.

And the other offices represented here today have shown similarly impressive returns on investment. Inspectors General ensure that Federal employees are not muzzled by their superiors when they challenge efforts to distort, misrepresent, or suppress scientific research and analysis. We are seeing increasing attempts by some special interests to keep agencies from reporting scientific data and studies on critical public health and safety issues. A couple come to mind: climate change and sea level rise.

Well, we shouldn’t stand for this suppression and hope none of you IGs will either. That is why late yesterday, 26 Senators, including many on this Committee, joined me in filing legislation to protect science and scientists from political interference. That’s why this Senator specifically inquired of the nominee for Secretary of Commerce as to his ideas on allowing free expressions in an agency where a lot of scientific analysis is given and where he has several Nobel Laureates that are employees.

This legislation that we filed would ensure that Federal scientists can communicate their findings to the public, the news media, and Congress. It also requires Federal agencies to implement and enforce scientific integrity policies and ensure procedures are in place to report when those integrity policies are broken. At the end of the day, inspectors general should play an important role in protecting whistleblowers who, in this particular example, believe scientific integrity has been compromised. But to carry out
these vital functions, they must have one thing, and that is independence.

Recently, The Washington Post and other news outlets reported that members of the administration’s transition team contacted a number of IGs and told them, according to The Washington Post, that they were “temporary holdovers” and may be replaced. Needless to say, this Senator found that news to be troubling, especially since Inspectors General have always been seen as independent entities that should only be removed for cause.

Last week, I sent letters to 11 IGs under this Committee’s jurisdiction to inquire further about the nature and extent of these transition team contacts and to learn more about each agency’s whistleblower policies. I’ve received responses from all 11 IGs. Both the DOT and DHS IGs have confirmed to me that they had been contacted by the transition team and initially informed that they would only serve on a temporary basis.

Mr. Chairman, I’d like to ask that these letters be entered into the record.

The CHAIRMAN. Without objection.

[The information referred to follows:]
Via Electronic Transmission

The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science
and Transportation
United States Senate

Dear Senator:

The following information is being transmitted in accordance with your request dated February 1, 2017. You requested information in response to the following questions:

1. How does the OIG educate agency employees about whistleblower protections? Please address how often the OIG provides training and what, if any, steps are taken to educate new agency employees. In addition, note whether training on the WPA and WPEA has occurred, or is scheduled to occur, for new appointees.

   a. The CPSC OIG does not provide direct training to employees about whistleblower protections. However, the CPSC OIG was instrumental in having the CPSC’s management provide training to CPSC employees and in having the CPSC comply with Office of Special Counsel (OSC) certification requirements regarding the Whistleblower Protection Enhancement Act. (See, https://ose.gov/Pages/Outreach/2302Cert.aspx).

   b. The CPSC is certified as complying with the Office of Special Counsel 2302(c) Agency Certification Program, required under the 2014 Whistleblower Protection Enhancement Act. (See, https://ose.gov/Pages/2302status.aspx.)

   c. In 2014, CPSC Acting Chairman Robert Adler designated Donna Simpson, the Director of Human Resources, as the Senior Accountable Government Official responsible for implementing the program.

d. To obtain OSC certification:

1. The CPSC posts informational posters on whistleblower protections and the 13 Prohibited Personnel Practices (PPPs) at agency facilities;

2. The CPSC provides new employees with information about whistleblower protections, including the 13 PPPs;

3. The CPSC provides employees with annual notices containing information about whistleblower protections;

4. The CPSC trains supervisors on whistleblower protections, including the 13 PPPs, every three years; and

5. The CPSC displays a link to OSC’s website on CPSC’s website or intranet.

e. Ms. Simpson sends annual notices of whistleblower protections to all agency employees. The most recent notice was sent on February 2, 2017.

f. Ms. Simpson confirmed to me by email that all supervisors completed the OSC required training on December 5, 2015. In accordance with OSC standards, the next supervisory whistleblower training is required to occur in 2018.

g. The CPSC’s Intranet provides links to OSC information on whistleblowing and prohibited personnel practices, under the Human Resources tabs. The CPSC OIG’s website provides information on whistleblower protections as well as a link to the OSC website. Additionally, it provides information to prospective complainants regarding their right to remain anonymous and be free from retaliation for contacting and/or cooperating with the Office of Inspector General.

2. Has the OIG sent a notice to agency employees after January 20, 2017, informing them of their rights under the WPA, WPEA, and other relevant statutes? If yes, provide a copy of the communication. If no, does OIG intend to send such a notice in the near future?

a. The OIG has not sent a notice to agency employees after January 20, 2017, informing them of their rights under the WPA, WPEA, and other relevant statutes.

b. However, the OIG has been in contact with senior agency management after January 20, 2017, regarding the need for outreach efforts to employees to ensure that they are aware of their rights, responsibilities, and the resources available to them. These outreach efforts will involve the OIG, the Office of General Counsel, Human Resources, and other relevant management officials.
c. As noted above, the CPSC’s Director of Human Resources did send a notice to all employees after January 20, 2017, informing them of their rights under the WPA and WPEA, providing information about the 13 PPPs, the rights of federal employees, the rights of federal employees who report wrongs, and contact information for the OIG and OSC. A copy of this communication is attached.

2. Have you designated a Whistleblower Protection Ombudsman? If yes, identify the individual and provide how long the individual has been in this position.

a. No. The designation of a Whistleblower Protection Ombudsman is required in offices of Inspector General whose IG is Presidentially appointed in accordance with section 3 of the Inspector General Act, but not by offices of Inspector General whose Inspectors General are not Presidentially appointed in accordance with section 8 of the Inspector General Act.

b. The CPSC OIG has considered the appointment of a Whistleblower Protection Ombudsman; however, given the size of the office, the only individuals technically qualified for the position would be conflicted from performing the duties of Ombudsman by their primary duties within the OIG.

4. Has your office been contacted by anyone associated with the Trump administration or transition team regarding the possibility of removal from your position as IG? If yes, was your office contacted again and reassured that you would not be forced from your position?

No, this office has not been contacted by anyone associated with the Trump administration or transition team regarding the possibility of removal from my position as IG.

Sincerely,

Christopher W. Dente

Attached: Annual Notice of Whistleblower Protections

cc: The Honorable John Thune, Chairman
Dentel, Christopher

From: Human Resources Management
Sent: Thursday, February 02, 2017 10:29 AM
To: Everyone - Fuel Only
Subject: Annual Notice of Whistleblower Protections

The purpose of this notice is to ensure that all agency employees are aware of and understand the prohibited personnel practices and whistleblower protections available to federal employees.

The December 5, 2013, White House National Action Plan calls for covered agencies to certify compliance with the Whistleblower Protection Act’s notification requirements. To that end, we have included below links to information about the U.S. Office of Special Counsel (OSC), which is an independent agency that protects federal employees from prohibited personnel practices, including whistleblower retaliation and unlawful hiring practices. OSC also provides an independent, secure channel for disclosing and resolving wrongdoing in federal agencies.

The Whistleblower Protection Act of 1989 and the Whistleblower Protection Enhancement Act of 2012 provide the right for all covered federal employees to make whistleblower disclosures and ensure that employees are protected from whistleblower retaliation. Whistleblowing is defined as the disclosure of information that an employee reasonably believes evidences: a violation of any law, rule or regulation; gross mismanagement; gross waste of funds; an abuse of authority; a substantial and specific danger to public health or safety; or censorship related to scientific research or analysis. Employees may make lawful disclosures to anyone, including, for example, management officials, the Inspector General of an agency, and/or OSC.

Please review the following fact sheet, “Your Rights as a Federal Employee,” which provides detailed information on the thirteen prohibited personnel practices and employees’ rights to file complaints with OSC. Additionally, I encourage you to review the following materials: “Know Your Rights When Reporting Wrong” and “The Role of the U.S. Office of Special Counsel,” which describe different avenues for making whistleblower disclosures and OSC’s role in accepting complaints from federal employees.

Federal employees have the right to be free from prohibited personnel practices, including retaliation for whistleblowing. This agency is committed to making sure that all employees are aware of their rights as well as the safeguards that are in place to protect them.
February 6, 2017

The Honorable Bill Nelson  
Ranking Member  
U.S. Senate  
Committee on Commerce, Science, and Transportation

Dear Ranking Member Nelson,

Thank you for your letter of February 1, 2017 seeking information from my office about our activities concerning whistleblowers and whistleblower protection. My office was established at the Corporation for Public Broadcasting (CPB) pursuant to the Inspector General Act amendments of 1988. My office is one of the Offices of Inspectors General (OIG) housed within entities that are not federal agencies. CPB is a District of Columbia non-profit corporation that receives a federal appropriation but is not a federal agency. Because CPB is not a federal agency, we have determined that CPB is not subject to the provisions of either the Whistleblower Protection Act of 1989 (WPA) or the Whistleblower Protection Enhancement Act of 2012 (WPEA).

We are, however, subject to the requirements of Section 7 of the Inspector General Act, which gives us the authority to receive and investigate complaints from agency employees and requires us, within certain parameters, to protect their identity. By internal policy, we provide whistleblower protection not only to CPB employee complaints but also, to the extent feasible, to complaints we receive from outside individuals, including the employees of CPB grantees like public radio and television stations. In addition to OIG policies that provide whistleblower protections, CPB has a whistleblower policy and other internal directives that recognize our authority to receive and review complaints and that require employees to report their good faith reasonable belief or suspicion of waste, fraud, abuse, or mismanagement.

We provide the following specific responses to the questions you presented:

1. How does the OIG educate agency employees about whistleblower protections? Please address how often the OIG provides training and what, if any, steps are taken to educate new agency employees. In addition, note whether training on the WPA and WPEA has occurred, or is scheduled to occur, for new appointees.

OIG has presented periodic voluntary anti-fraud training for CPB employees, part of which includes informing employees of the authority of the OIG to receive complaints and for employees to remain confidential and/or anonymous. The General Counsel of CPB conducts an annual ethics briefing for all CPB employees and that briefing includes
2. Has the OIG sent a notice to agency employees after January 20, 2017, informing them of their rights under the WPA, WPEA, and other relevant statutes? If yes, provide a copy of the communication. If no, does OIG intend to send such a notice in the near future?

OIG has not sent a notice to CPB employees. As noted above, CPB is not subject to the provisions of the WPA or the WPEA. We plan to work with CPB's President to develop a joint message to all CPB employees to remind them of the importance of cooperating with the OIG, including the responsibility to provide timely access to information and documentation, and their whistleblower rights and responsibilities.

3. Have you designated a Whistleblower Protection Ombudsman? If yes, identify the individual and provide how long the individual has been in this position.

OIG has not designated a Whistleblower Protection Ombudsman, because CPB is not subject to the WPEA.

4. Has your office been contacted by anyone associated with the Trump administration or transition team regarding the possibility of removal from your position as IG? If yes, was your office contacted again and reassured that you would not be forced from your position?

I have not been contacted by the Trump administration or transition team.

Thank you for the opportunity to provide you with this information. My office has been and will continue to be very supportive of anyone who presents us with information about fraud, waste, abuse, or mismanagement. Pursuant to the Inspector General Act and our internal policies, we provide confidentiality to complainants who specifically ask for confidentiality and we routinely ask complainants who do not make a specific request if they want their identity or information to be handled with confidentiality.

If you have any questions or concerns about this response, please feel free to contact me at mmitchelsson@cpb.gov or 202-879-9628 or my Counsel, Helen Mollick, at hmollick@cpb.gov or 202-879-9616.

Sincerely yours,

Mary Mitchellson

cc: The Honorable John Thune, Chairman
February 6, 2017

The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science and Transportation
United States Senate
Washington, DC 20510-6125

Dear Ranking Member Nelson:

This is in response to your letter to the Department of Transportation (DOT) Office of Inspector General (OIG) dated February 1, 2017, regarding whistleblower protections and recent news reports about Inspectors General and the presidential transition team. Specifically, you requested information on:

1) education and training for current and new DOT employees,
2) notification since January 20, 2017, to DOT employees about their whistleblower rights,
3) OIG's designated Whistleblower Protection Ombudsman, and
4) recent communications with the presidential transition team regarding my position.

Education and Training of Current and New Employees

Our Web site provides DOT employees with substantial information about their whistleblower rights and remedies related to allegations of retaliation. The Web site provides information about the Whistleblower Protection Ombudsman, the purpose of the Ombudsman, and his contact information. The Web site discusses several aspects of whistleblower retaliation—what it means to make a protected disclosure, the types of personnel actions covered by the statutes, the processes for pursuing a whistleblower retaliation claim, and potential remedies. It further explains that DOT employees may file a claim of whistleblower retaliation with OIG or with the Office of Special Counsel (OSC) and offers contact information for DOT's Whistleblower Protection Ombudsman. Additionally, contact information for OSC's Complaint Center Operations (CCO), and links to OSC's Web site are available directly from our Web site. Further, OSC has certified OIG under 5 U.S.C. § 2302(c) for compliance with its obligations to inform DOT's workforce of their rights and remedies under the prohibited personnel practice and

4 www.oig.dot.gov/whistleblower

CC207008
whistleblower protection provisions of chapters 12 and 23 of Title 5. This certification is effective through December 2017.

In addition to OIG’s certification, nearly all DOT administrations have been certified by OSC for compliance with section 2302(e). These administrations are the Office of the Secretary, Federal Aviation Administration, Federal Highway Administration, Federal Motor Carrier Safety Administration, Federal Railroad Administration, Maritime Administration, and Pipeline and Hazardous Materials Safety Administration. The National Highway Traffic Safety Administration and Saint Lawrence Seaway Development Corporation have registered with OSC for the certification program as well. The Federal Transit Administration (FTA) has provided whistleblower training and materials to its employees but has not yet registered with OSC. However, FTA’s Executive Director has assured OIG that it will register with OSC and complete the certification process.

Along with having a Whistleblower Protection Ombudsman, OIG investigative field offices refer potential whistleblower retaliation complainants to the Ombudsman. OIG’s processes inform DOT employees of OSC’s primary jurisdiction to investigate whistleblower retaliation complaints. When DOT employees contact OIG’s CCO alleging whistleblower retaliation, they receive information about OSC, including the OSC intake unit’s phone number and address. Since January 1, 2015, CCO has referred 17 potential complainants to OSC.

All OIG employees receive training on whistleblower retaliation laws and protections. During new employee orientation, OIG staff receive a presentation on whistleblower retaliation rights and remedies. OIG also educates its employees about their whistleblower rights as part of its mandatory training under the Notification and Federal Anti-Discrimination and Retaliation Act of 2002, commonly called the No FEAR Act.

**Notification of Whistleblower Protections**

We have not yet sent a notice to DOT employees since January 20, 2017, to inform them about their whistleblower retaliation rights. However, OIG plans to contact each DOT Operating Administration shortly to offer training and materials to ensure that DOT employees remain cognizant of their whistleblower protections.

**Designated Whistleblower Protection Ombudsman**

Attorney-Investigator Jason Weidenfeld has been designated by my office as DOT’s Whistleblower Protection Ombudsman since January 2016. Prior to OIG, he worked for OSC from April 2002 to October 2015.

Contact: CCO

Connaughton 07/03/18
Contacts from the President-Elect's Transition Team Regarding the IG's Position

I was contacted via email by a representative of the President-elect's transition team for DOT on the night of Friday, January 13, 2017, and informed that I was being "held over on a temporary basis." The next day I responded via email acknowledging receipt of the notice. The transition team representative responded to let me know that if I needed anything I was free to call anytime and included a cell phone number. Subsequently, on Wednesday, January 18, 2017, I initiated a face-to-face discussion with the same transition team representative regarding the January 13 email notification. During this discussion, the transition team representative gave what I understood to be a reassurance that I would continue to serve as DOT's Inspector General.

If I can answer any additional questions or be of further assistance, please contact me at (202) 366-1959 or Nathan Richmond, Director and Counsel, Office of Congressional and External Affairs, at (202) 493-0422.

Sincerely,

Calvin L. Scovel III
Inspector General

cc: The Honorable John Thune, Chairman
February 6, 2017

The Honorable Bill Nelson
Ranking Member
Committee on Commerce,
Science, and Transportation
United States Senate
Washington, D.C. 20510

Via Electronic Mail to:
Brad Tourney at brad.tourney@commerce.senate.gov
Muneer Ahin at muneer.ahin@commerce.senate.gov
Jason Van Net at Jason.VanNet@commerce.senate.gov
Adolfo Pani at Adolfo.Pani@commerce.senate.gov

Dear Senator Nelson:

This letter responds to your request for information dated February 1, 2017, regarding Office of Inspector General efforts to inform agency employees about whistleblower protections. Our responses are numbered in accordance with your questions:

1. How does OIG educate agency employees about whistleblower protections? Please address how often OIG provides training and what, if any, steps are taken to educate new agency employees. In addition, note whether training on the WPA and WPLA has occurred, or is scheduled to occur, for new employees.

The FCC requires all employees to complete a training module every two years on the provisions of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act) including training on prohibited personnel actions and whistleblower disclosures. Employees were required to complete the most recent training by October 1, 2016. All new employees are required to take the training as part of their FCC orientation activities.

Further, the FCC OIG maintains a general hotline that is publicized on the FCC public-facing website (https://www.fcc.gov/office-inspector-general/hotline) to facilitate the -1-
reporting of allegations of fraud, waste, abuse, or mismanagement within Federal Communications Commission (FCC) programs or operations. The website informs whistleblowers that allegations may be reported by FCC employees, FCC contractors, or the general public. While not specifically citing to the WPA, the website notes that OIG will protect the identity of individuals reporting allegations to the maximum extent possible by law. Confidentiality for FCC employees is established by Section 7(b) of the Inspector General (IG) Act of 1978, which precludes the IG from disclosing the identity of a FCC employee who reports an allegation or provides information, without the employee's consent, unless the IG determines that disclosure is unavoidable during the course of the investigation. Non-FCC employees who report allegations may specifically request confidentiality.

2. Has the OIG sent a notice to agency employees after January 20, 2017, informing them of their rights under the WPA, WPEA, and other relevant statutes? If yes, provide a copy of the communications. If no, does OIG intend to send such a notice in the near future?

We have not sent such a notice and currently do not plan to do so.

3. Have you designated a Whistleblower Protection Ombudsman?

The FCC OIG has not designated a Whistleblower Protection Ombudsman. We have taken the position that because the requirement is contained in section 3(d)(XCVII) of the IG Act, it applies only to Presidentially Appointed IGs and not to Designated Entity IGs, such as the FCC IG, enumerated in Section 8 of the IG Act.

4. Has your office been contacted by anyone associated with the Trump administration or transition team regarding the possibility of removal from your position as IG?

Neither I, nor to my knowledge, anyone else in my office, has been contacted by anyone associated with the Trump administration or transition team regarding the possibility of removal from my position as IG.

Thank you for your continued interest in and support of my office and the Inspector General community. Please do not hesitate to call me at (202) 418-1222 or Jay C. Keilholz, Assistant Inspector General Investigations/Counsel to Inspector General at (202) 418-2319 if you have any questions.

Sincerely,

David L. Haggerty
Inspector General

c: The Honorable John Thune, Chairman
Dear Ranking Member Bill Nelson:

In your letter dated February 1, 2017, you requested information on the Federal Maritime Commission (FMC) Office of Inspector General’s (OIG) activities to inform the agency’s employees about whistleblower protections. The FMC OIG appreciates your support and recognition of the important role Inspectors General (IGs) play in combating fraud, waste, and abuse at our federal agencies. Further, my office recognizes the importance of whistleblowers’ disclosures and the protections afforded to them under a number of laws passed by Congress. My office is committed to being an agent of positive change for the FMC, and in that regard, I welcome any feedback you may have on these matters.

Please find the answers to your questions below.

1. How does the OIG educate agency employees about whistleblower protections? Please address how often the OIG provides training and what, if any, steps are taken to educate new agency employees. In addition, note whether training on the WPA and WPEA has occurred, or is scheduled to occur, for new appointees.

Answer: The OIG educates agency employees about whistleblower protections in several ways. First, OIG-specific training is provided during the new employee orientation briefings held by the OIG. At these briefings, the OIG meets with new employees, provides the new employees a copy of the OIG information brochure, and talks about the mission of the OIG and the complaint process. The OIG brochure provides guidance on the protections afforded to complainants, and specifically cites the Whistleblower Protection Act (WPA) that prohibits reprisals for complaining or cooperating with the OIG. This OIG brochure is available electronically online; in the OIG office and distributed to new employees of the agency. The OIG’s brochure references the OIG’s website, where additional information can be found online regarding the Whistleblower Protection Enhancement Act of 2012 (WPEA).
In addition, both the FMC OIG and the agency have each obtained the Office of Special Counsel (OSC) 2302(c) certification. To receive OSC certification, the FMC OIG and the agency were required to complete the five certification requirements, to include:

1. Place informational posters at FMC facilities;
2. Provide information to current employees about the 13 prohibited personnel practices (PPPs) and whistleblower disclosures to new employees as part of the orientation process; and
3. Display a link to OSC's website on the OIG's and agency's websites.

Lastly, the FMC does not have new appointees, and therefore training for new appointees has not been needed. The FMC is an independent regulatory agency directed by five Commissioners appointed for staggered five-year terms, with one Commissioner designated by the President to serve as Chairman. The Chairman is the Chief Executive and Administrative Officer of the agency. When a change in appointees does occur, the OIG will schedule a new employee briefing, to include training on the WPA and WPEA. Please be advised that new employees of current appointees receive the OIG training during their new employee orientation.

2. Has the OIG sent a notice to agency employees after January 20, 2017, informing them of their rights under the WPA, WPEA, and other relevant statutes? If yes, provide a copy of the communication. If no, does OIG intend to send such a notice in the near future?

Answer: Yes, the OIG sent a notice to agency employees on February 6, 2017 informing them of their rights under the WPA, WPEA, and other relevant statutes. Please find attached a copy of the notice.

3. Have you designated a Whistleblower Protection Ombudsman? If yes, identify the individual and provide how long the individual has been in this position.

Answer: No, the FMC OIG has not established a Whistleblower Protection Ombudsman. The FMC OIG reads the WPA as requiring only that Presidentially-appointed IGs appoint an Ombudsman. Specifically, Section 117 of the WPA, Whistleblower Protection Ombudsman, amends section 3 of the Inspector General Act of 1978 (5 U.S.C. App.). Among other provisions, section 3 of the Inspector General Act provides for the appointment and removal of Inspectors General by the President, but does not specifically mention designated federal entity (DFE) IGs in this section. The FMC OIG is a DFE and the IG is appointed by the FMC's agency head (the Commissioner).
4. Has your office been contacted by anyone associated with the Trump administration or transition team regarding the possibility of removal from your position as IG? If yes, was your office contacted again and reassured that you would not be forced from your position?

Answer: No.

If I can provide you with any further information, please do not hesitate to contact me at (202) 523-0863 or via email at jhatfield@fmc.gov.

Sincerely,

[Signature]

Jon Hatfield
Inspector General
Federal Maritime Commission

Attachment

cc: The Honorable John Thune, Chairman
Good afternoon FMC staff,

From time to time, it is appropriate for the Office of Inspector General (OIG) to remind employees that they play an important role in the OIG’s mission to prevent and detect fraud, waste, and abuse in the FMC’s programs. In addition, Congress has recognized the importance of whistleblowers and has afforded them protections under a number of laws which are discussed below.

Office of Inspector General

Reports concerning wrongdoing in the FMC programs should be submitted directly to the OIG Hotline (https://www2.fmc.gov/oigcomplaints/). The OIG does not share its Hotline records with FMC officials, and the Inspector General Act, as amended, provides for a prohibition on the disclosure of the identity of an individual who disclosed information to an OIG Hotline. The Inspector General Act, in addition to the Whistleblower Protection Act, provides protection against the retaliation of an employee who complains or cooperates with the OIG. Please review the OIG’s brochure for more information on the OIG mission and other helpful information.

Whistleblower Protection/Prohibited Personnel Practices

The Whistleblower Protection Act of 1989 and the Whistleblower Protection Enhancement Act of 2012 provide the right for all covered federal employees to make whistleblower disclosures and ensure that employees are protected from whistleblower retaliation. Whistleblowing is defined as the disclosure of information that an employee reasonably believes evidences: a violation of any law, rule or regulation; gross mismanagement; gross waste of funds; an abuse of authority; a substantial and specific danger to public health or safety; or censorship related to scientific research or analysis. Employees may make lawful disclosures to anyone, including, for example, management officials, the Inspector General of an agency, and/or the Office of Special Counsel (OSC).

Please review the following fact sheet, “Your Rights as a Federal Employee,” which provides detailed information on the thirteen prohibited personnel practices and employees’ rights to file complaints with OSC. Additionally, I encourage you to review “Know Your Rights When Reporting Wrongs,” which describe different avenues for making whistleblower disclosures as federal employees. More information can also be found on the OSC website, including several informative videos.

How to File Whistleblower Retaliation Complaints

If an adverse personnel action has been taken or threatened against you in retaliation for making a disclosure of wrongdoing to the OIG, or elsewhere, you may submit a complaint to the OIG Hotline, and/or to the U.S. Office of Special Counsel. Allegations of retaliation regarding EEO matters generally should be addressed through the EEO process.

If you have any questions or concerns, please contact me, (202)523-5863, jhatfield@fmc.gov, or feel free to stop by the OIG. Thank you.
February 7, 2017

The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science
and Transportation
United States Senate
Washington, DC 20510

Dear Senator Nelson:

This letter responds to your letter of February 1, 2017, which requested information regarding the Office of Inspector General’s efforts to inform Amtrak employees about whistleblower protections. The information below corresponds to the four questions listed in your letter.

As context, Amtrak’s federal status is unique inasmuch as Congress created it in 1970 as a “for profit” organization. As such, it is not a federal department or agency, and its personnel are not Federal employees under Title 5 of the U.S. Code. While Amtrak is subject to many federal oversight laws and regulations, the “for profit” non-federal organizational characterization has been a consistent theme in subsequent revisions and reforms to Amtrak’s enabling legislation.

Consequently, Amtrak’s employees are not covered by the Whistleblower Protection Act (WPA) or the Whistleblower Protection and Enhancement Act (WPEA)—laws that are specifically linked to federal employment status. Amtrak employees are however, covered by whistleblower protections external to Title 5’s framework, such as the Federal Railroad Safety Act, which is implemented through the Department of Labor’s Occupational Safety and Health Administration. Accordingly, we support this legislation—which informs potential whistleblowers of workplace protections under the law, encourages disclosure of wrongdoing, and offers protection from retaliation.

1. Our office provides regular briefings to Amtrak employees to, among other things, bring awareness to the importance of reporting instances of fraud, waste, and abuse. As part of these briefings, our presenters regularly discuss protections available for individuals reporting wrongdoing. In the last two fiscal years, our office provided 85 presentations to nearly 1000 Amtrak employees. In addition, our Relationship Policy with Amtrak details specific protections.
available to whistleblowers and our external website—which is linked on Amtrak’s Internet and employee Intranet—contains information on whistleblower protection. Amtrak also includes whistleblower protection information on their employee Intranet.

2. As noted above, Amtrak employees are not covered by the WPA or the WPEA. Accordingly, we do not notify Amtrak employees of the WPA, WPEA, or other Title 5 related statutes, as they are not applicable to them.

3. Our office has not designated a Whistleblower Protection Ombudsman, as this requirement flows from the WPEA and is not applicable to Amtrak. Nevertheless, education about whistleblower protection is a key function of the Office of Inspector General, and we continue to review ways to improve that role.

4. Our office has not been contacted by anyone associated with the Trump administration or transition team regarding the possibility of my removal from the position of Inspector General.

If you have any questions, please contact me or Kevin Wintens, Deputy Inspector General/Counsel, at 202-906-4600.

Sincerely,

[Signature]

Tom Howard
Inspector General

cc: The Honorable John Thune, Chairman
    Committee on Commerce, Science and Transportation
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security
Washington, DC 20528 / www.oig.dhs.gov

February 7, 2017

The Honorable Bill Nelson, Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate
Washington, DC 20510

Dear Ranking Member Nelson:

Thank you for your February 1, 2017 letter requesting information about the Department of Homeland Security, Office of Inspector General’s (DHS OIG) efforts to inform DHS employees about whistleblower protections. We share your views about the important role whistleblowers play in combating fraud, waste, and abuse within an agency, and acknowledge that none of the work we do at the OIG is possible without the men and women in the DHS workforce, as well as DHS contractors, coming forward to report incidents of potential misconduct.

We have raised our profile within DHS as the entity to which whistleblower complaints are reported, and with effective results. It is our duty to protect these individuals from being retaliated against as a result of stepping forward and, as before, we remain committed to empowering and protecting agency whistleblowers. We are grateful for the opportunity to share with you information about how the DHS OIG educates agency employees about the rights and protections afforded whistleblowers under the Whistleblower Protection Act (WPA), Whistleblower Protection Enhancement Act of 2012 (WPEA), and other relevant statutes.

1. The DHS OIG educates all new agency employees about whistleblower protections shortly after they join the agency. The OIG Whistleblower Protection Ombudsman (WPO), who has primary responsibility for whistleblower protection training and education within the agency, provides WPA and WPEA training to all new DHS headquarters employees at the new employee orientations presented twice monthly by the DHS Chief Human Capital Office (CHCO). The WPO provides new employees an overview of his role and responsibilities, describes the elements
of whistleblower protection and prohibited personnel practices, and educates the employees on their rights. At the training, new employees are provided with handouts prepared by the Office of Special Counsel (OSC) on each of these topics. DHS is in the process of scheduling training for new appointees, which will include OIG training on the WPA and WPEA.

Beyond the training received as part of new employee onboarding, each DHS employee must also complete No Fear Act training every two years, which provides training on employees' rights and remedies under whistleblower protection and anti-discrimination laws. DHS employees in a supervisory role also receive additional whistleblower protection training.

The WPO works closely with the DHS Under Secretary of Management's Office, the DHS CHCO, the DHS Chief Leadership Officer Council, and the individual training officers at each DHS component agency to address whistleblower protections. He collaborates with these groups on the role of the Ombudsman in DHS, the development of training materials for all employees through the DHS OIG website, and the delivery of mandatory whistleblower training materials to new and existing employees through the DHS learning management system.

The WPO works directly with OSC to ensure that the OIG is providing DHS employees and supervisors with the most current whistleblower protection training. In Fiscal Year 2016, the WPO, working with OSC, provided supervisory training on the WPA and WPEA that fulfilled the necessary requirements to achieve OSC 2302e certification for the DHS OIG. The OIG then worked to achieve certification for the entire Department. Training for this certification required all 26,000 DHS supervisors to complete online OSC training and pass an online quiz. The WPO then worked with CHCO to convert the quiz into the DHS learning management system, where it is now required training for supervisors every three years.

2. The OIG will send a notice to all agency employees informing them of their rights under the WPA, WPEA, and other relevant statutes shortly. A copy of the draft notice is enclosed herewith.

3. The OIG appointed Senior Executive James Gaughran as the OIG WPO on October 1, 2015. Previously, Mr. Gaughran spent
twenty plus years as a Special Agent with the United States Secret Service, serving in the Presidential Protection Division for Presidents Carter and Reagan and as a “Legislative Fellow” at the U.S. House of Representatives. In 1998, Mr. Gaughran joined the IG community. He came to DHS OIG in 2008, serving as the Principal Deputy Assistant IG for Investigations and Emergency Management Oversight before taking on the role of OIG WPO in 2015.

4. I was contacted on the evening of January 13, 2017 by the head of President-Elect Trump’s DHS transition team and informed that I would continue to serve as DHS Inspector General only on a “temporary” basis following the inauguration. I was encouraged to look for alternative employment. I pressed for a reasoning for this decision, but the head of the transition team said he was just passing a message given by the higher ups and did not have any insight into it. After reaching out to the Council of the Inspectors General on Integrity and Efficiency, as well as contacts on several of the Senate and House committees to which the OIG reports, I learned that I would be permitted to remain in my role following the inauguration. I am honored to continue to serve as the DHS IG, and am focused on the important work ahead of us.

Finally, given your interest in whistleblower protection, I wanted to highlight some important changes in the way the DHS OIG performs its whistleblower protection function. In the last year, we undertook a substantial reorganization and rebuilding of this function by creating a new and dedicated Whistleblower Protection Unit (WPU) housed in our Office of Counsel (OC). The WPU consists of the WPO, a supervisory whistleblower investigator, and two newly hired whistleblower administrative investigators. The WPU has primarily been responsible for intake and preliminary complaint review during this timeframe, while OC attorneys and Special Agents from the DHS OIG Office of Investigations jointly conduct all whistleblower investigations that are opened.

We are confident these changes will make us more effective, though we acknowledge that it will take constant vigilance and dedicated effort to ensure that whistleblowers with claims of retaliation are heard, and that their claims are fairly and independently investigated.

I appreciate your interest in ensuring that the OIG is educating DHS employees about whistleblower protection laws. Please call me with any
questions, or your staff may contact Diana Shaw or Rachel Magnus,
Congressional Liaisons, Office of Legislative Affairs, at (202) 254-4100.

Sincerely,

John Roth
Inspector General

Enclosure

cc: The Honorable John Thune, Chairman
Subject: Reporting fraud, waste, and abuse; whistleblower protection

During this time of transition within the Department of Homeland Security, I wanted to take a moment of your time to reintroduce the Office of Inspector General to the DHS community. The DHS has a critical mission. Like you, the men and women in OIG are dedicated to the mission and want to work with you to help the Department be more effective and efficient.

One of the ways we do this is through investigations, audits, and inspections. Some of our best work has been the result of conscientious and dedicated DHS public servants who have provided us information that has resulted in saving DHS millions of dollars, or stopped ethically questionable activity. We very much appreciate your assistance.

By taking a proactive role in improving DHS by reporting wrongdoing, you can root out waste, fraud, and abuse. We have a number of ways to report information, but the most efficient is to use our OIG Hotline. The hotline is a resource for you to report allegations of civil rights and civil liberties abuses, employee corruption, ethics violations, prohibited personnel practices, program fraud and financial crimes, and other criminal and non-criminal activity associated with waste, abuse or fraud. Basically, if you see something that is not right within DHS, and it affects the DHS mission, you should feel free to report it. Go to our website: http://www.oig.dhs.gov/index.php.

You have the right to remain anonymous, although we are able to more fully investigate your claim if you identify yourself. The Inspector General Act and the Whistleblower Protection Act give the Inspector General powerful legal tools both to protect your identity and to ensure that you are not retaliated against for reporting allegations. I take my obligation to protect whistleblowers very seriously. We have had hundreds of individuals report matters to us, and we have an outstanding track record in ensuring that your identity is protected.

A key element of our commitment to protecting whistleblower activity is the Office of Inspector General's Whistleblower Protection Unit. This Unit, through the Whistleblower Ombudsman, ensures Department employees and contractors are aware of the role and importance of whistleblowers in improving the effectiveness and efficiency of the Department's operations and educates them on their legal rights and protections against retaliation. We also alert Department officials and managers to the possible repercussions of retaliation against those who make protected disclosures.

Additionally, our Whistleblower Protection Unit and investigators working with the Unit:

- Promptly and thoroughly review every complaint of retaliation for whistleblowing activity received through the OIG hotline;
- Investigate and report on specific cases of whistleblower retaliation by DHS employees;
- Communicate with whistleblowers about the status and resolution by the OIG of those complaints.
Serve as the OIG liaison to other U.S. agencies with whistleblower responsibilities, such as the Office of Special Counsel, and to non-governmental whistleblower organizations and advocacy groups.

Additional information regarding your rights as a whistleblower, the types of disclosures that are protected, and the complaint process is available on our website at https://www.oig.dhs.gov/index.php?option=com_content&view=article&id=136:whistleblower-resources&catid=16:fasttrack&Itemid=146 or on the website of the Office of Special Counsel at https://osc.gov/.

Again, thanks to all of those who have had the courage to step forward to help us. Together, we can make sure that DHS fulfills its mission to the American people.

John Roth
Inspector General
February 07, 2017

The Honorable Bill Nelson
Ranking Member
U.S. Senate Committee on Commerce, Science and Transportation
254 Russell Senate Office Building
Washington, D.C. 20510

Dear Senator Nelson:

Thank you for your letter of February 1, 2017, regarding the Whistleblower Protection program for the Office of Inspector General (OIG) at the U.S. Department of Commerce (DOC).

In response to your question regarding our training for the Department’s current and new employees as well as new appointees, in Fiscal Year 2016, the Whistleblower Protection Ombudsperson (WPO) conducted 17 outreach and training sessions with internal and external DOC operating units. Additionally 58 employees contacted the WPO directly with questions regarding whistleblower protections. Other whistleblower protection activities included the publication of a “Frequently Asked Questions” on the OIG’s website. The DOC OIG also sent out two notices to agency employees informing them of their rights under the Whistleblower Protection Act (WPA), Whistleblower Protection Enhancement Act (WPEA), and other relevant statutes in June 2015 and January 2016, respectively. We plan to distribute whistleblower protection informational packets to new political appointees no later than February 28, 2017, or as they come onboard. With regard to new employee training, the OIG participates in the bi-weekly new hire orientations provided by the Department. At each orientation, the OIG presents a briefing on whistleblower protections.

You asked if the OIG sent a notice to employees after January 29, 2017, informing them of their rights under the WPA, WPEA, and other relevant statutes. According to our WPO implementation plan for Fiscal Year 2017, our plan is to send a communication to DOC employees and contractors on or around July 30, 2017, in recognition of National Whistleblower Day.

In response to your question regarding our Whistleblower Protection Ombudsperson, Cecelia Wilson is the WPO for our office. She was selected for this position in October 2015 after the prior WPO transferred to another agency.

Regarding your inquiry whether my office was contacted by the Trump administration or transition team regarding the possibility of my removal as Inspector General, we were not contacted regarding this issue.

Please let me know if you have any questions.

Sincerely,

[Signature]
Inspector General
February 7, 2017

VIA ELECTRONIC TRANSMISSION

The Honorable Bill Nelson
Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
425 Hart Senate Office Building
Washington, DC 20510

Dear Ranking Member Nelson:

Thank you for your February 1, 2017, letter and for the efforts of the Committee on Commerce, Science, and Transportation to support the Federal Trade Commission (FTC) Office of Inspector General (OIG) and its role in ensuring employee whistleblower protections. Please find my Office’s response below:

1. How does the OIG educate agency employees about whistleblower protections? Please address how often the OIG provides training and what, if any, steps are taken to educate new agency employees. In addition, note whether training on the WPA and WPEA has occurred, or is scheduled to occur, for new appointees.

The OIG educates new FTC employees about the whistleblower protections mandated by the Whistleblower Protection Act of 1989 (WPA) and the Whistleblower Protection Enhancement Act of 2012 (WPEA) in numerous ways. We participate on the weekly new employee orientation sessions required for all new FTC employees, excluding political appointees, and our presentation includes a segment on whistleblower responsibilities and protections, including the prohibition against retaliation. These trainings also provide instructions on how to file a complaint. Similar presentations are also provided at the FTC University (FTC-U) training provided to new FTC employees within their first year of employment, as well as during the OIG’s regional outreach visits to the FTC’s regional offices. We also provide new employees an educational trifold that summarizes these rights and protections. Further, we participate on the training panel for the FTC’s supervisory development program for new supervisors, and our segment provides a similar overview and information geared toward supervisor responsibilities and prohibitions. Political appointees are invited to these trainings but are not required to attend.
Additionally, the OIG, in collaboration with the FTC’s Office of General Counsel and Human Capital Management Office, issues an annual memorandum to all FTC employees, including political appointees, to educate staff on their whistleblower rights and remedies. The memorandum is issued as part of the FTC’s registration process for the Office of Special Counsel’s (OSC) 2302(c) certification program, which “allows federal agencies to meet the statutory obligation to inform their workforce about the rights and remedies available to them under the prohibited personnel practice and whistleblower retaliation protection provisions of 5 U.S.C. § 2302.”

Moreover, all new employees, including political appointees, are required to receive No Fear Act training within 90 days of onboarding. These trainings, which are conducted by the FTC’s Equal Employment Opportunity Office, include a segment on the whistleblower protection.

2. Has the OIG sent a notice to agency employees after January 20, 2017, informing them of their rights under the WPA, WPEA, and other relevant statutes? If yes, provide a copy of the communication. If not, does OIG intend to send such a notice in the near future?

Yes. On February 6, 2017, the OIG sent a notice to agency employees reminding them of their rights under the WPA, WPEA, and other relevant statutes. A copy of the relevant portion of the notice is attached. Additionally, the OIG is a co-signatory on the annual whistleblower rights and protection notice issued to staff per the OSC 2302(c) certification requirements. The previous notice was issued on May 9, 2016, and we expect to issue the next annual notice in the spring.

3. Have you designated a Whistleblower Protection Ombudsman? If yes, identify the individual and provide how long the individual has been in this position.

The OIG has interpreted the WPEA and its amendments to section 3(d)(1)(C) of the Inspector General Act of 1978, as amended, with respect to designating a Whistleblower Protection Ombudsman to apply only to the Presidentially-appointed OIGs, and not to the Designated Federal Entity OIGs, such as the FTC OIG. Therefore, the FTC OIG does not have a designated Whistleblower Protection Ombudsman. As a micro-sized OIG, we have found it to be effective and efficient to receive whistleblower complaints through the OIG hotlines, the OIG email address, mail, and fax. Per OIG policy, the Administrative Assistant assigns the complaints a complaint number, logs them, and forwards them to the two OIG investigators for review and further action, as appropriate. The OIG also receives in-person referrals, and the intake process for such matters is coordinated by the investigators. All FTC employees are educated on how to file whistleblower complaints through the various trainings listed in our response to question # 1 above.

4. Has your office been contacted by anyone associated with the Trump administration or transition team regarding the possibility of removal from your position as IG? If yes, was your office contacted again and reassured that you would not be forced from your position?

Yes. I received a voicemail in our general office mailbox on Friday, January 13, 2017, stating that
the President Elect's FTC Transition Landing Team Lead wished to speak with me. I attempted to
return the call on Monday, January 16, 2017, and left a voicemail message. The Landing Team
Lead called back and left a second voicemail message that day stating, in substance, that he had
been asked to call me with a specific question, but that "the issue has been addressed" and therefore
he did not need to speak with me. He thanked me for meeting with him and the Landing Team
earlier in the month. I have had no further communication with anyone associated with the
President Elect's FTC Transition Team or the new administration on this topic.
If you have any questions, please do not hesitate to call me at 202-326-3527.

Sincerely,

Rosalyn A. Mazer
Inspector General

cc: The Honorable John Thune
Chairman
February 6, 2017

Whistleblower Protections for Federal Employees

The Office of Inspector General (OIG) reminds FTC employees that federal law prohibits governmental personnel from retaliating against an employee who acts as a whistleblower by reporting suspected waste, fraud, or abuse to the OIG. Agency officials may not take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment because the employees disclosed information which they reasonably believe is evidence of (1) a violation of any law, rule, or regulation, or (2) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, so long as the disclosure is not specifically prohibited by law or Executive Order.

Whistleblower Retaliation is personnel action in response to a protected disclosure of information and includes actions that could adversely affect the whistleblower, such as:

- A non-promotion
- A disciplinary action
- A detail, transfer or reassignment
- An unfavorable performance evaluation
- A decision concerning pay, benefits or awards
- A significant change in duties, responsibilities or working conditions

Employees have many lawful options for reporting whistleblower complaints, including to management officials, the OIG, and the Office of Special Counsel (OSC). Complaints of retaliation can be reported to the OIG, OSC, or any other employee designated by the agency head to receive such disclosures. Employees may contact the OIG Hotline at 1-800-FTC-HELP, call 202-326-2800, or contact anyone in the OIG. Please visit the OIG web page for additional information about whistleblower protections.
The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science, and Transportation
Washington, D.C. 20510-6125

February 7, 2017

Dear Senator Nelson:

I am writing in response to your February 1, 2017, letter regarding the National Science Foundation (NSF) Office of Inspector General’s (OIG) efforts to inform the agency’s employees about whistleblower protections.

With respect to your first question, NSF OIG educates agency employees about whistleblower protections in a variety of ways. NSF brings on new employees almost every pay period and holds a 2-day New Employee Orientation (NEO) program for each incoming group. OIG representatives present at each of these NEOs. Featured within the OIG presentation delivered at each NEO is a discussion of whistleblower rights and protections under the WPA and the WPEA.

In addition to these sessions, at every elevator bank on every floor in both NSF buildings there is a glass case containing a large document with detailed descriptions of whistleblowing, whistleblower retaliation (including actions that can be taken if whistleblower retaliation occurs), and how to contact the Office of Special Counsel (OSC). The OIG webpage also provides a link to a page which provides specific information about the WPA and the WPEA and how to contact NSF’s Whistleblower Ombudsman. Finally, after obtaining our own certificate of compliance with 5 U.S.C. §2302(c) from OSC several years ago, we helped NSF management obtain a similar certificate. To retain this certification, NSF must provide annual OSC-related training, which includes a discussion of whistleblower protections, to all employees.

In response to your question about the education of new appointees, it is important to remember that all appointees at NSF (the NSF Director, Deputy Director and the members of the National Science Board) are term appointees. As of the date of this letter, all those positions except that of the NSF Deputy Director are currently filled. When new appointees arrive at NSF, we will ensure that they are informed about NSF’s Whistleblower Ombudsman and the protections afforded by the WPA and the WPEA.

In response to your second question, my office has not sent a notice to agency employees after January 20, 2017, about whistleblower protections. Given the many ways in which information related to whistleblower protections is shared across the Foundation, we have not identified a need to send a separate notice.
In response to your third question, William Kilgallin, senior advisor in the Office of Investigations, has been the NSF OIG whistleblower protection ombudsman since January 2013.

Finally, I received no contact from anyone associated with the administration or the transition team indicating that I might be removed as Inspector General.

If you have any questions, or need additional information, please call me or Ken Chason, Counsel to the Inspector General, at 703-292-7100.

Sincerely,

Allison C. Lerner

cc: The Honorable John Thune, Chairman
The Honorable Bill Nelson  
Ranking Member  
Committee on Commerce, Science, and Transportation  
United States Senate  
Washington, DC 20510  

February 8, 2017  

Dear Ranking Member Nelson:  

The NASA Office of Inspector General (OIG) shares your strong interest in protecting agency whistleblowers from retaliation for protected disclosures. In addition, we appreciate your support of the OIG and our role in providing independent oversight of NASA personnel and activities.  

In a February 1 letter to this office, you raised three questions about our whistleblower activities and a question about transition issues at the OIG. Our answers to each are below:  

1. How does the OIG educate agency employees about whistleblower protections? Please address how often the OIG provides training and what, if any, steps are taken to educate new agency employees. In addition, note whether training on the WPA and WPEA has occurred, or is scheduled to occur, for new appointees.  

We maintain a Whistleblower Protection Ombudsman webpage where NASA employees and the public may access information about Federal whistleblower protections. In addition, we issue an annual notice to all NASA employees about whistleblower protection and the cooperation with OIG investigations and audits we expect from the Agency and its managers. We sent our most recent notice on May 19, 2016. In addition, the OIG Whistleblower Protection Ombudsman gave a presentation on whistleblower retaliation to NASA employees in June 2015 at their Annual Agency Ombudsmen meeting at NASA Headquarters.  

Last year, the NASA OIG obtained 5 USC 2302(c) certification from the United States Office of Special Counsel. This certification evidences that NASA OIG met the statutory obligation to inform its workforce about the rights and remedies available to them under
the Civil Service Reform Act, the WPA, and the WPEA, as well as to meet the requirements of the second Open Government National Action Plan. As part of that certification process, OIG attorneys presented training on prohibited personnel practices (including whistleblower retaliation) to all OIG supervisors and auditors. We have also trained our investigators, who investigate allegations of whistleblower retaliation against employees of certain federal contractors and subcontractors, on federal whistleblower protection law.

We understand NASA is in the process of seeking 2302(c) certification for the Agency as a whole and is planning on-line training for all employees as part of the process. We have coordinated with NASA’s Office of Human Capital Resources on this training.

2. Has the OIG sent a notice to agency employees after January 20, 2017, informing them of their rights under the WPA, WPEA, and other relevant statutes? If yes, provide a copy of the communication. If no, does OIG intend to send such a notice in the near future?

As noted above, we issue an annual notice to all NASA employees regarding their rights under the Whistleblower Protection Act. This year’s notice will go out in the Spring of this year. In addition, at our request the former Administrator twice over the past several years sent a notice informing NASA employees of their duty to cooperate with the OIG. The most recent notice included the following language:

In addition, every NASA employee has a responsibility to cooperate with OIG audits and investigations, including by providing prompt and complete access to agency information, documents, and personnel. And as a reminder, it is illegal for managers to retaliate against employees for bringing information to or cooperating with the OIG.

We plan to ask the incoming Administrator to issue a similar notice once he or she is confirmed.

3. Have you designated a Whistleblower Protection Ombudsman? If yes, identify the individual and provide how long the individual has been in this position.

Frank LaRocca, Counsel to the Inspector General, has served as the OIG’s Whistleblower Protection Ombudsman since November 2012.

4. Has your office been contacted by anyone associated with the Trump administration or transition team regarding the possibility of removal from your position as IG? If yes, was your office contacted again and reassured that you would not be forced from your position?

No, the NASA Inspector General was not contacted by the transition team about the possibility of removal.
Please contact me or Renee Jahans, the OIG's Executive Officer, if you have questions or require additional information.

Sincerely,

Paul K. Martin
Inspector General

cc: The Honorable John Thune
Chairman
Committee on Commerce, Science, and Transportation
United States Senate
So during today’s hearing, it’s my hope that we can learn more about how we can ensure the independence of these offices. I also look forward to hearing how the Inspectors General will work to ensure that the integrity of the scientific process is protected.

So, thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Nelson.

We’ll move to our panel, and I want to start on my left and your right with Ms. Lerner, and then we’ll move to Ms. Gustafson, Mr. Roth, and Mr. Scovel. If you could confine your stated public remarks to as much as 5 minutes, that would be great. Anything else will get put into the record and we’ll get to our questions.

So, Ms. Lerner, please proceed.

STATEMENT OF ALLISON C. LERNER, INSPECTOR GENERAL, NATIONAL SCIENCE FOUNDATION

Ms. LERNER. Thank you. Mr. Chairman and members of the Committee, I appreciate this chance to discuss some of the top management challenges facing the National Science Foundation. As requested, my testimony will focus on areas that pose the highest risk of accountability to NSF: management of cooperative agreements for large facility research projects, management of the Inter-governmental Personnel Act Program, and the U.S. Antarctic Program, and improving grant administration.

NSF uses cooperative agreements to construct and operate its most costly and highest-risk research facilities. As of January 2017, NSF has 22 cooperative agreements valued at over $50 million each and totaling over $4.4 billion. Since 2010, my office has issued 28 reports containing more than 80 recommendations related to NSF’s use and management of these agreements for large facilities.

Our work has demonstrated that the need for strong oversight of large facility cooperative agreements extends over the life cycle of such awards. Pre-award oversight should include audits of proposed budgets and accounting systems to ensure that awardees’ cost estimates are fair and reasonable and that the entity’s accounting system is adequate to bill the government properly.

Once an award has been made, we have recommended incurred cost submissions and audits. Such actions help ensure that costs being claimed by awardees are consistent with Federal requirements and enable NSF to identify and address problematic or fraudulent charges as early as possible.

NSF has developed policies and procedures for large facilities awards to address some OIG recommendations, including guidance requiring an analysis of proposed costs for each large facility before an award is made to determine if the costs are adequately supported and a new management fee policy to strengthen oversight of the use of such fees. These new policies represent important steps toward accomplishing the goal of increased accountability over the Foundation’s largest and riskiest projects, and they contributed to the removal of a longstanding significant deficiency in this year’s financial statement audit.

Given this progress, our ongoing work will focus in part on how NSF is applying its new policies. Implementing them will require sustained management attention; effective communication with the awardee community; clear award terms and conditions; and, most
importantly, a continuing commitment to change the culture at NSF. We will also pay close attention to the Foundation’s actions in response to the American Innovation and Competitiveness Act, which contains a number of key oversight requirements related to NSF’s large facilities.

To advance its mission of supporting science and engineering research and education, NSF brings in temporary personnel under the Intergovernmental Personnel Act for rotational assignments of up to 4 years. Since individuals serve in a temporary capacity, there is significant turnover in staff at NSF, especially in executive positions charged with leading the Foundation and setting its vision.

The Foundation’s use of IPAs also comes at a high cost. In 2015, NSF paid nearly $8.9 million for 27 executive level IPAs. Such IPAs can also earn substantially more than Federal employees. In 2015, the highest paid executive level IPA salary was $440,000.

NSF has begun to take steps to reduce IPA costs. Among other things, it no longer reimburses IPAs for lost consulting income. We plan to examine NSF’s actions in response to both our recommendations and provisions of the Competitiveness Act which focuses on IPAs.

Management of the U.S. Antarctic Program and NSF’s Antarctic Support Contract is a continuing challenge. In recent reports, we have recommended ways for NSF to improve oversight of the health and safety of participants in the USAP and to prioritize and track its actions in response to the 2012 Blue Ribbon Panel report. We plan to be onsite in Antarctica in January 2018 to conduct field work for the 2017 audits of NSF’s financial statements and its information security program.

Ensuring that grant funds are spent as intended is essential to NSF’s mission. Because many NSF awardees pass portions of their funding on to subrecipients, we have recently started an audit of NSF’s process to ensure that its awardees are appropriately monitoring their subrecipients. We plan to share our findings with Congress in December 2017.

Finally, we continue to monitor challenges associated with NSF’s move this year to its new headquarters in Alexandria, Virginia. We’ll provide updates as we identify risks.

A key contributor to the progress the Foundation has made in responding to our office’s work is the Stewardship Collaborative, which was established by NSF and OIG in 2010 as a collective effort to help achieve the shared mission of proper stewardship of the taxpayers’ investment in science. My office will continue to utilize the full range of our audit and investigative resources to exercise robust oversight of NSF’s stewardship of Federal funds and to safeguard the integrity of the Foundation’s operations.

Public trust and confidence demand the highest level of accountability, and we look forward to working with NSF management, the National Science Board, and Congress to achieve this goal.

Thank you.
Mr. Chairman and Members of the Committee, I appreciate this opportunity to discuss the Office of Inspector General’s (OIG) work to promote the efficiency and effectiveness of the National Science Foundation’s (NSF) programs and operations and to safeguard their integrity. My office is committed to providing rigorous, independent oversight of NSF, and I welcome the chance to discuss some of the top management challenges facing the Foundation, NSF’s progress in addressing these challenges, and work that remains to further advance accountability and transparency at NSF.

Background

NSF is an independent Federal agency and the funding source for approximately 24 percent of all federally supported basic research conducted by the Nation’s colleges and universities. In many areas, such as mathematics and computer science, NSF is the major source of Federal backing. The Foundation funds approximately 12,000 new awards each year, thereby fulfilling its mission to promote the progress of science. Proposals for funding are assessed by panels of experts as part of NSF’s merit review process.

Awards are made primarily as grants to individuals and small groups of investigators, as well as to research centers and facilities where scientists, engineers, and students undertake research projects. The Foundation also uses cooperative agreements and contracts to fund major research equipment such as telescopes, Antarctic research sites, and high-end computer facilities. In FY 2016 NSF was appropriated approximately $7.5 billion to carry out the Foundation’s programs and operations.

The OIG is independent from NSF and reports directly to Congress and the National Science Board (NSB). Our mission is to conduct independent and objective audits, inspections, reviews and investigations of National Science Foundation programs and operations, and to recommend policies and corrective actions to promote effectiveness and efficiency and prevent and detect waste, fraud, and abuse. Consistent with our statutory mandate, the OIG has an oversight role and does not determine policy or in management activities involving the Foundation or program operations. Thus, my office is not responsible for managing any NSF programs, nor do we attempt to assess the scientific merit of research funded by the Foundation.

The OIG has two main components: the Office of Audit and the Office of Investigations. The Office of Audit is responsible for auditing NSF’s internal operations, as well as the grants, contracts, and cooperative agreements funded by the Foundation. Among its ongoing responsibilities are the annual audits of NSF’s financial statements and the annual reviews of NSF’s information system security program.

Through our audit work, we are able to monitor management functions that may pose significant financial or programmatic risks to the Foundation. In determining priorities for this work, we consider the results of prior audits and consult with the Foundation’s senior management, the National Science Board and Congress, the Office of Management and Budget, and members of the research community supported by the Foundation. In selecting areas for audit, we assess factors such as the risk involved in the activity, the potential for monetary recovery for the government, and the potential for the greatest substantive benefit for NSF.

The Office of Investigations (OI) is responsible for investigating allegations of wrongdoing involving NSF programs and operations, agency personnel, and organizations or individuals who submit proposals to, receive awards from, or conduct business with NSF. OI also houses a team of investigative scientists responsible for investigating allegations of fabrication, falsification or plagiarism in NSF-funded research. We focus our investigative resources on the most serious cases, as measured by such factors as the amount of money involved, the seriousness of the alleged criminal, civil or ethical violations, and the strength of the evidence. When appropriate, the results of these investigations are referred to the Department of Justice for possible criminal prosecution or civil litigation, or to NSF for administrative resolution.

NSF’s Top Management Challenges

In accordance with the Reports Consolidation Act of 2000, each year the OIG identifies what it considers to be the most serious management and performance challenges facing NSF. The top management challenges reflect fundamental program risk that are likely to require NSF’s attention for years to come.

The OIG identified seven challenges for NSF for FY 2017. My testimony will focus on four of NSF’s most pressing challenges: management of cooperative agreements for large facility research projects, management of the Intergovernmental Personnel Act program, management of the U.S. Antarctic Program, and improving grant ad-
ministration. I will also briefly discuss risks associated with NSF’s move to its new building, which is scheduled to begin toward the end of this Fiscal Year.

Management of Cooperative Agreements for Large Facility Research Projects

NSF uses cooperative agreements to construct and operate its most costly and highest risk research facilities. As of January 25, 2017, NSF had 459 active cooperative agreements, totaling nearly $8 billion. Twenty-two of these agreements are valued at over $50 million each and add up to cumulatively to more than $4.4 billion.

Since 2010, my office has issued 28 reports containing more than 80 recommendations related to NSF’s use and management of cooperative agreements for the construction and operation of its high-dollar, high-risk research facilities. Monitoring of cooperative agreements was also cited as a significant deficiency in NSF’s financial statement audits for Fiscal Years 2011 through 2015.

In addition to OIG’s oversight, in the spring of 2015, at the request of the NSF Director and the National Science Board, the National Academy of Public Administration (NAPA) examined NSF’s use of cooperative agreements for large facilities and benchmarked its practices against other, similar Federal agencies.

NAPA issued its report in December 2015. That document articulated the fundamental challenge that NSF is facing:

It is clear that, in the past, NSF has prioritized the innovative scientific aspects of large facility construction projects; the agency now needs to apply equal emphasis on increased internal management of the business practices critical to enhanced oversight and project success. In doing so, the Panel believes that NSF and NSB will enhance the agency’s ability to fulfill its mission of supporting groundbreaking science.

The need for stronger oversight of large cooperative agreements begins before the award has been made. Pre-award oversight should include audits of proposed budgets and accounting systems to ensure that awardees’ cost estimates are fair and reasonable and that their accounting systems are adequate to bill the government properly. Pre-award oversight is especially important as the proposed budget for these projects, once approved by NSF, creates the basis upon which awardees can draw down advanced funds over the course of the award.

The importance of pre-award oversight was underscored by the results of audits of three of NSF’s large facility projects—the Ocean Observatories Initiative (OOI), the Daniel K. Inouye Solar Telescope (DKIST), and the National Ecological Observatory Network (NEON). As a result of those jobs, auditors questioned $305 million in unallowable or unsupported costs out of $1.1 billion in total costs for the three projects.

The lack of support for costs in the $469.3 million NEON proposal was so significant that the auditors issued an adverse opinion stating the proposal did not form an acceptable basis for negotiation of a fair and reasonable price. Auditors disclaimed an opinion on the DKIST proposal, concluding that cost data provided in the pre-award cost proposal for the $344 million project was so significantly flawed that they were unable to perform an audit. Based on these audits, we recommended that prior to making an award NSF obtain proposal and accounting system audits for high risk cooperative agreements valued in excess of $50 million. The NAPA report also recommended that NSF address potential cost proposal issues before making an award.

The serious questions about the adequacy of the proposed budgets led us to examine NSF’s cost surveillance throughout the lifecycle of large facility projects. Adequate oversight is essential after the award is made to ensure that expenditures are consistent with the award’s terms and conditions. To this end, we have recommended that NSF obtain incurred cost submissions and incurred cost audits of high risk cooperative agreements valued in excess of $50 million. Such submissions and audits will enable NSF to determine if costs claimed are reasonable and allowable under Federal requirements.

Proper oversight also includes validating the information awardees provide in Earned Value Management (EVM) reports and certifying the EVM systems used to track project schedule and cost. Our work has identified opportunities for improvement in this area. For example, monthly EVM progress reports for the NEON project were not accurate, which undermined NSF’s ability to promptly identify problems that ultimately led to NSF having to significantly de-scope the project to avoid an $80 million cost overrun.

1National Science Foundation: Use of Cooperative Agreements to Support Large Scale Investment in Research, National Academy of Public Administration (December 2015), pp. 6–7.
2Formerly known as the Advanced Technology Solar Telescope.
We are currently broadening our work in this area to encompass cooperative agreements for the operations phase of large facility projects. Over time, NSF spends significantly more on operating its facilities than it does on constructing them. To illustrate, NSF requested over $193 million for Fiscal Year 2017 to pay for four NSF large facility construction projects. In contrast, NSF’s operation and maintenance request for its existing large facilities for the same time period exceeded $1 billion, in addition to more than $200 million for Federally Funded Research and Development Centers. We have just begun a job focusing on the risk of potential commingling of construction and operations funds.

NSF has developed new policies and procedures for large facility awards to address some OIG and NAPA recommendations. Among other things, NSF’s new guidance requires completion of a Cost Proposal Review Document (CPRD) for each large facility proposal to ensure that a thorough and well-documented record exists of NSF’s determination that proposed costs are reasonable. The CPRD is NSF’s analysis of whether an awardee’s proposed costs are supported adequately and describes NSF’s plans for oversight of the award.

In addition, according to NSF’s new guidance, the Grants and Agreements Officer must determine that a project’s estimated costs are reasonable prior to making a construction award for a facility. NSF has also instituted a new management fee policy, as well as implementing guidance, to strengthen its oversight over awardees’ use of management fee.

These new policies represent important steps by NSF toward the goal of increased accountability over the Foundation’s largest and riskiest projects. As a result of these actions, NSF’s most recent financial statement audit removed a multi-year significant deficiency focused on NSF’s monitoring of large cooperative agreements. While these outcomes reflect real progress on this important issue, we will continue to monitor this area because of the unique challenges it poses to the Foundation.

Based on the serious nature of these challenges and the progress that has been made to date, our objective moving forward is to examine how NSF is applying its new policies to strengthen accountability for both construction and operations awards from the pre-award stage through the lifecycle of the award. Implementing these new policies will require sustained management attention, effective communication with the awardee community, clear award terms and conditions, and most importantly, a continuing commitment to change culture at NSF.

We will also pay close attention to the actions NSF takes in response to requirements in the American Innovation and Competitiveness Act. The Act contains a number of key oversight requirements related to NSF’s large facility portfolio. For instance, it requires NSF to conduct a pre-award analysis of costs before making an award, obtain periodic external reviews on project management and performance, retain control over funds budgeted for contingency, and to establish guidelines regarding inappropriate expenditures associated with all fee types.

Management of the Intergovernmental Personnel Program

To further the agency’s mission of supporting science and engineering research and education, NSF draws on scientists, engineers, and educators on rotational assignment from academia, industry, or other eligible organizations. All of the non-permanent appointments are Federal employees with the exception of those who come to NSF under Intergovernmental Personnel Act (IPA) assignments. Individuals on IPA appointments remain employees of their home institutions. As a result, pay and benefits for IPAs are set by their home institutions and are not subject to limitations on Federal pay and benefits.

While there are benefits that come from having IPAs at NSF, there are also challenges. For example, since IPAs can serve in a temporary capacity for up to four years, there is significant turnover in staff at NSF, especially in executive positions charged with leading the Foundation and setting its vision. As of December 2016, five of the seven Assistant Directors, whose primary responsibility is providing leadership and direction to the Foundation’s scientific directorates, are IPAs (one Assistant Director slot is vacant). In addition, as of the same date, 20 out of NSF’s 29 scientific divisions are led by IPAs (2 of those positions are vacant).

The Foundation’s use of IPAs comes at a high cost and these costs are rising. In 2015, NSF paid nearly $8.9 million for 27 executive-level IPAs, compared to $6.5 million for the same expenses for 21 executive-level IPAs in 2012. IPA salaries can also significantly exceed the salaries of the highest paid Federal employees. In 2015 the highest executive-level IPA salary was more than $440,000, up 45 percent from $301,247 in 2012. In 2015 the salaries for all but two executive level IPAs were more than the highest salary of a Federal employee at NSF. The number of IPAs

2Includes salary, fringe benefits, lost consulting, and per diem.
In August 2016, Leidos Holdings Inc. and Lockheed Martin’s Information Systems and Global Solutions business segment merged. As a result of the merger, Leidos will hold the Antarctic Support Contract, once plans for all contracts affected by the merger have been reviewed.

has also increased—in 2009, there were 20 executive-level IPAs, whereas there were 29 executive-level IPAs in December 2016.

Since 2010, we have recommended that NSF evaluate ways to reduce IPA costs and have suggested, among other things, that the Foundation consider expanding the use of telework and seek greater cost sharing from IPAs' home institutions. Because IPA salaries and benefits are funded with program-related appropriations, savings in IPA costs would free up funds for additional research.

In response to our recommendations NSF no longer reimburses IPAs for lost consulting income; previously IPAs could receive up to $10,000 from NSF each year for consulting income they received while at their institutions. NSF also formed a steering committee in April 2016 to explore opportunities to reduce IPA costs. To this end, NSF has indicated that it will pilot a required 10 percent cost sharing of IPAs’ academic-year salary and fringe benefits in FY 2017.

Moving forward, we will monitor NSF’s actions in response to our recommendations on this topic. We will also examine NSF’s actions in response to the American Innovation and Competitiveness Act, which required the Foundation to report on its efforts to cut costs associated with employing IPAs.

Management of the U.S. Antarctic Program

NSF, through the United States Antarctic Program (USAP), manages U.S. scientific research in Antarctica. In December 2011, NSF awarded an Antarctic Support Contract to Lockheed Martin to support NSF’s management of the USAP.† The contract is NSF’s largest, valued at nearly $2 billion over 13 years. The Antarctic Support Contract and its subcontracts provide logistical support for information technology, food, laboratory management, and other services which enable the USAP’s three research stations (McMurdo, South Pole, and Palmer) to operate year round.

We have previously examined NSF’s response to a July 2012 Blue Ribbon Panel report and suggested that including more specific information, such as interim milestones and target dates for implementing actions, would enhance NSF’s ability to prioritize and track its corrective actions in response to the Panel report. Given the large number of action items associated with the Panel recommendations—the panel identified 84 implementing actions within three separate categories—there is a real risk that NSF could lose track of its progress with respect to these actions unless it approaches implementation systematically.

We have also examined NSF’s oversight of and the Antarctic Support Contractor’s actions to ensure the health and safety of participants in the USAP. We found that in general NSF’s oversight and the Contractor’s performance were effective in ensuring adequate health and safety. We also identified four areas for improvement, including the lack of a process for identifying, responding to, and tracking data on misconduct that occurs in the USAP, and opportunities to enhance pharmacy operations.

In January 2018 we plan to visit the McMurdo and South Pole research stations to conduct fieldwork for the 2017 financial statement audit, the 2017 audit of NSF’s information security program, and other aspects of the USAP program as appropriate.

Improving Grant Administration

Making grants in support of promising scientific research is central to NSF’s mission. Thus, ensuring that grant funds are spent as intended is critical. While efforts to reduce the administrative burden on grantees have value, the agency must proceed carefully so that accountability for public funds is not compromised in the process.

Because many NSF awardees pass portions of their funding on to subrecipients that perform a significant amount of the project’s work, NSF must ensure that such awardees are appropriately overseeing the actions and expenditures of their subrecipients. We have recently started an audit on NSF’s process to ensure that its awardees are monitoring their subrecipients and, pursuant to the American Innovation and Competitiveness Act, we will provide our report and any associated recommendations, to Congress no later than December 2017.

Moving NSF Headquarters to a New Building

NSF has four months (September through December 2017) to complete its move from the two buildings it currently occupies in Arlington, Virginia, to its new head-
quarters in Alexandria, Virginia, and decommission its current offices before its current leases expire at the end of December, 2017. If the current offices are not decommissioned prior to January 1, 2018, the Foundation will have to begin paying possibly increased rent for the Arlington offices, in addition to rent for its new Alexandria location. Our most recent examination of risks associated with NSF’s move recommended that NSF improve its baseline schedule, which could play a critical role in NSF’s ability to identify and manage project risk.

NSF management informed us that it does not intend to update its baseline schedule and proposed an alternative approach that relies on its existing schedule. We will continue to closely monitor NSF’s progress toward meeting the deadline to move and will provide updates to the agency and the Congress as we identify risks.

**NSF and OIG Efforts to Strengthen Accountability**

As noted previously, the Foundation has begun to make progress in its efforts to achieve greater accountability. A key contribution to the progress to date has been made by the Stewardship Collaborative, a group which was established by NSF and OIG in 2010 as a collective effort by both offices to help achieve the shared mission of proper stewardship of the taxpayer’s investment in science, engineering, and education.

The Collaborative is made up of members from varying units within NSF and OIG and is chaired by Senior Executive leaders from NSF’s financial administration division and OIG’s Office of Audit. It meets monthly to discuss current issues and possible upcoming barriers to resolution—as well as potential solutions. For example, it recently developed a joint training effort to improve understanding of the audit resolution process, including members’ responsibilities in the process.

Along with increasing positive communication, the Collaborative has been instrumental in resolving a number of critical audit recommendations. Most importantly, it has helped ensure that NSF has addressed recommendations without impinging on the OIG’s independence and that management decisions are made by the right people within the Foundation.

**Conclusion**

Scientific research and discovery are the building blocks of the technological advances that are essential for our Nation’s economy to grow and to meet the challenges of the future, and NSF has an essential role to play in promoting scientific discovery. For the agency to achieve its mission, NSF must spend its research funds in the most effective and efficient manner while maintaining the highest level of accountability over taxpayer dollars.

My office will continue to utilize the full range of our audit and investigative resources to exercise robust oversight of NSF’s stewardship of Federal funds and to safeguard the integrity of the Foundation’s operations. NSF applies its highest level of attention and scrutiny to its financial management of its programs and operations. Public trust and confidence demand the highest level of accountability, and we look forward to working with NSF management, the National Science Board, and Congress to achieve this goal.

The CHAIRMAN. Thank you, Ms. Lerner.
We’ll now turn to the Honorable Peggy Gustafson.

**STATEMENT OF HON. PEGGY E. GUSTAFSON, INSPECTOR GENERAL, U.S. DEPARTMENT OF COMMERCE**

Ms. GUSTAFSON. Chairman Thune, Ranking Member Nelson, and members of the Committee, I very much appreciate the opportunity to testify today about the Department of Commerce’s top management and performance challenges.

In my more than 7 years of being an IG in Federal Government, it is very clear that it is extremely helpful when Congress calls up the IGs and asks us to discuss our work, because the agency pays a lot of attention when it knows that Congress is asking us about our work. So I appreciate being called up here at the beginning of this Congress, this administration, at the beginning of my tenure as Commerce IG.
My testimony today is going to focus on some of the areas discussed in our most recent top management challenges report covering Fiscal Year 2017.

Chairman Thune, as you noted, with the passage of the Middle Class Tax Relief and Job Creation Act of 2012, FirstNet was established as an independent entity within the National Telecommunications and Information Administration. NTIA’s mission is to create and operate the first high-speed nationwide wireless broadband network for public safety at all levels. So far, FirstNet’s significant challenges have been managing the complex acquisitions inherent in the network, estimated to cost tens of billions of dollars once it is built; successfully consulting with state and local public safety entities and strengthening their internal controls as our office and other independent auditors identify issues in need of correction action.

To date, FirstNet has been provided with approximately $7 billion in funding, as provided in its enabling legislation. As FirstNet has grown and been built up, its expenditures have continued to increase as it moves toward building this network. In 2012, FirstNet spent less than $250,000, and by 2015, it had spent $49 million in expenditures. But, of course, these represent only the tip of the iceberg.

FirstNet’s significant spending is going to begin this year in earnest, when it awards the most significant contract that is going to be awarded to a partner who will work with FirstNet to build this network envisioned in the original legislation. And, again, everybody anticipates that this network is going to cost tens of billions of dollars. We are committed to providing oversight during this critical stage of this deployment.

To date, our work has focused on FirstNet’s efforts related to internal control and its consultations with stakeholders on the network features, but our future work is going to be dependent on FirstNet’s post-award activities. It may include oversight of FirstNet’s management of state network plans, issues related to its geographical coverage, or the management of the contract itself. As you noted, Senator Thune, we will continue to adjust our oversight approach as FirstNet grows and as its challenges become greater.

Another major challenge facing the Department is that the National Oceanic and Atmospheric Administration must manage the risks of its satellite acquisition and development. NOAA’s environmental satellite programs represent about one-sixth of the Department’s more than $9 billion budget. NOAA must continue to manage the acquisition and development risks of the satellite systems as they develop and launch the next generation of weather satellites.

NOAA had delayed the launch of its geostationary satellite, GOES-R, numerous times before its November 2016 launch. This delay and other delays create risks of coverage gaps in weather information as the existing NOAA satellites reach the end of their design life.

Another NOAA challenge and a fourth major issue is balancing the priorities of the fishing industry and its multiple stakeholders. NOAA Fisheries must balance the competing factors of promoting commercial and recreational fishing while preserving the popu-
lations of fish and marine life. As Congress has increasingly looked into NOAA’s Fisheries management, our office has planned oversight work on related issues, such as a survey of scientific assessments that NOAA uses to estimate the populations of various fish stocks.

Another area I would like to mention briefly is the creation of a Department-wide culture of accountability. The Department of Commerce’s goal of operational excellence requires management’s attention to its computer systems as well as other Department-wide risk factors. Under an audit we performed pursuant to the Cybersecurity Act of 2015, we identified significant challenges related to strengthening the national security systems. We understand the Department is now addressing the risks associated with its national security systems, but cybersecurity will certainly be an issue that remains on our radar and as a focus of our work.

In 2016, our Office of Investigations processed more than 500 complaints regarding departmental operations. We opened more than 80 investigations into allegations of fraud, waste, and abuse and closed more than 50 investigations. Almost half of these investigations resulted in criminal convictions, suspensions or debarment, or disciplinary actions.

The last thing I want to focus on very quickly is the efficiency and effectiveness of the Department’s operations. We are committed to ensuring that the Department resolves and implements each recommendation that is included in our products. Since Fiscal Year 2015, we have provided more than 200 recommendations to the Department. For the recommendations listed in Fiscal Year 2015, two-thirds have been implemented; and for the recommendations made in 2016, this rate is currently around one-third.

I would note that Mr. Ross in his confirmation hearing talked about the need to address the outstanding issues related to our reports, and should he be confirmed, I am very much looking forward to working with him and the other leadership of the Department to make sure that these reports are addressed and these recommendations are getting closed.

Thank you very much.

[The prepared statement of Ms. Gustafson follows:]
Challenge 1. TRADE AND INVESTMENT—Expand the U.S. economy through increased exports and foreign direct investment that leads to more and better American jobs.

Challenge 2. INNOVATION—Foster a more innovative U.S. economy—one that is better at inventing, improving, and commercializing products and technologies that lead to higher productivity and competitiveness.

Challenge 3. ENVIRONMENT—Ensure communities and businesses have the necessary information, products, and services to prepare for and prosper in a changing environment.

Challenge 4. DATA—Improve government, business, and community decisions and knowledge by transforming Department data capabilities and supporting a data-enabled economy.

Challenge 5. OPERATIONAL EXCELLENCE—Strengthen the Department’s capacity to achieve its objectives, maximize return on program investments, and deliver quality, timely service.

The challenges I will highlight today focus on the following areas:

1. the First Responder Network Authority (FirstNet)
2. the National Telecommunications and Information Administration (NTIA)
3. National Oceanic and Atmospheric Administration (NOAA) satellites
4. NOAA Fisheries
5. oversight of the Department’s management and spending
6. OIG recommendations issued to the Department of Commerce

I. FirstNet

Addressing the challenges of ensuring the successful procurement and monitoring of a nationwide high-speed, broadband network dedicated to public safety

FirstNet, created by the Middle Class Tax Relief and Job Creation Act of 2012 (the Act), is an independent authority within NTIA. The law gives FirstNet the mission to build, operate, and maintain the first high-speed, nationwide wireless broadband network dedicated to public safety at the local, state, tribal, and Federal levels. FirstNet will provide a single interoperable platform for emergency and daily public safety communications.2

The program currently operates with no appropriated funds other than those initially borrowed. The Federal Communications Commission (FCC) sold by auction valuable spectrum to the public in FYs 2014 and 2015. Of the $45 billion raised, $6.8 billion was provided to FirstNet in FY 2015 to build a network on retained spectrum. Currently, the program has $6.5 billion on hand.

FirstNet's most significant challenges to date concern managing its acquisitions, consulting with public safety entities at all levels, and strengthening internal control.

Effective management of acquisitions. In January 2016, FirstNet issued a request for proposals (RFP) for the development, building, and management of a National Public Safety Broadband Network (NPSBN). Proposals were due May 31, 2016, and FirstNet—with assistance from the Department of Interior’s Acquisitions Services Directorate—evaluated proposals to select the best vendor solution. The award will be delayed due to a protest by an unsuccessful bidder. In its RFP, FirstNet adopted an objectives-based approach—rather than a traditional requirements-driven model—to help industry develop innovative solutions for the NPSBN. The successful bid must meet the objective-based goals of the RFP. Also, as the RFP points out, FirstNet must provide services at competitive prices, given constrained local, state, and Federal budgets. Further, FirstNet must be self-sustaining—by leveraging existing infrastructure, maximizing value for excess network capacity, and optimizing its pricing structure.

The contractor selected will be awarded a contract billion to build a cellular network dedicated to first responders. Once complete, it is estimated that the network could cost $25–50 billion, all of which will be covered by the contractor—which will build and maintain the network, working with all 56 states and territories. The contractor will also implement either the FirstNet plan or integrate the state-approved plan. Other contractor responsibilities will include managing revenues, costs, and paying yearly fees to FirstNet.

Effective consultation with states and localities. FirstNet is required by the Act to consult with the 56 states and territories, as well as tribes and Federal public safety entities, in order to build and deploy an effective NPSBN.\textsuperscript{3} NTIA issued \$116.56 million in grant awards under the Act’s State and Local Implementation Program (SLIGP) to promote associated outreach, data collection, and planning for the NPSBN. Nearly all entities were consulted to discuss priority and preemption (i.e., moving commercial users off the network in an emergency), coverage for large events, rural coverage, and what users will pay for the service. States and territories provided network coverage feedback for developing state plans.

To realize a nationwide design that meets public safety needs, FirstNet must continue to work with designated points-of-contact at each location and entity and develop individual state plans for building and deploying radio access networks. FirstNet will provide a coverage plan for each state and territory or, if the plan is not found acceptable, the state can provide its own. If a state opts out of FirstNet, and uses its own coverage plan, that state’s plan will still be required to tie into FirstNet’s backbone system—and it will pay for the FirstNet service. Plans will be submitted to FCC for approval.

Continue to strengthen internal control. Reports issued by OIG,\textsuperscript{4} the Government Accountability Office,\textsuperscript{5} and an independent public accounting firm\textsuperscript{6} have identified the need for FirstNet to strengthen its controls. Our recent audit of FirstNet’s management of its interagency agreements (IAAs) found that FirstNet could strengthen controls regarding documenting IAA tracking and closeout procedures; we also noted that FirstNet could maintain readily available documentation and provide timely responses to audit requests to demonstrate transparency and accountability of programs and operations.\textsuperscript{7}

A FirstNet–OIG memorandum of understanding (MOU) funded at \$1.35 million was developed in FY 2014 to address lack of an oversight provision in FirstNet legislation. This MOU was cancelled in July 2016, and now OIG funds its FirstNet oversight with its base appropriation.

II. NTIA

Addressing increased demand for radio frequency spectrum and implementing a replacement system to modernize, automate, and integrate key spectrum management functions

NTIA must address the increasing demand for radio frequency spectrum through sharing among Federal and commercial entities. It will accomplish this mission through expanding broadband Internet access and adoption, expanding the use of spectrum, and ensuring the Internet is an engine for economic growth.

Freeing up radio frequency spectrum to meet the increasing demand for high-speed broadband services—while ensuring no loss of critical existing and planned federal, state, local, and tribal government capabilities—remains a key challenge facing the Department. In June 2010, the President directed the Department, working through NTIA, to make 500 megahertz of Federal and non-federal spectrum available by 2020 to support wireless broadband needs.\textsuperscript{8} In June 2013, Federal agencies were further directed to expand the availability of spectrum by accelerating efforts to share Federal spectrum with non-federal users.\textsuperscript{9}

\textsuperscript{3}47 U.S.C. § 1426(b)(1).
\textsuperscript{9}The White House Office of the Press Secretary, June 14, 2013. “Expanding America’s Leadership in Wireless Innovation,” Memorandum for the Heads of Executive Departments and Agencies [online].
According to the most recent report— as of June 2016, or 6 years after the President’s 2010 directive and with 4 years remaining to achieve the goal—NTIA reported that it has made 245 megahertz of spectrum available, which is almost half of the 500 megahertz goal. NTIA continues to investigate opportunities to make additional spectrum available by conducting studies, consulting with the Federal Communications Commission, and undertaking research and development (R&D) activities to better understand spectrum-sharing capabilities between Federal and non-Federal users. Additionally, NTIA continues to search for a replacement system for the Federal Spectrum Management System (FSMS), which was terminated in 2015.

FSMS was intended to support Federal spectrum management by (1) identifying and managing spectrum for Federal use and (2) identifying and releasing spectrum for non-Federal use.

As the 2020 target approaches, NTIA’s challenge is to incorporate lessons learned from its R&D activities and consultation efforts into actual strategies that lead to more efficient use and availability of radio frequency spectrum. Also, the termination of FSMS necessitates that the Department identify a technological system that can modernize, automate, and integrate key spectrum management functions.

Ongoing OIG oversight. Our ongoing work includes

- **NTIA Management of the State and Local Implementation Grant Program (SLIGP).** This $135 million grant program supports state level efforts to plan for the implementation of FirstNet. We anticipate issuing our final report in FY 2017.
- **NTIA Oversight of Grant Award to the Los Angeles Regional Interoperable Communications System (LA–RICS).** This $154 million Broadband Technology Opportunities Program (BTOP) grantee has entered into an initial 5-year spectrum lease agreement with FirstNet, allowing it to provide wireless communication services to public safety entities. For this audit initiated in FY 2017, we will assess LA–RICS’ efforts to meet grant objectives and provide the FirstNet with lessons learned.

### III. NOAA Satellites

Managing environmental satellite system acquisition and development risks

The Department must manage risks associated with the acquisition and development of environmental satellite systems. NOAA’s major satellite system programs are among the Department’s largest investments, totaling more than 16 percent of its $9.7 billion FY 2017 budget request.

NOAA geostationary and polar-orbiting environmental satellites provide some of the most important data and imagery for weather forecasting and storm tracking. After a number of delays, NOAA’s GOES–R program launched its first satellite—GOES–16—on November 19, 2016. The month before, NOAA announced that the JPSS program would delay the launch of JPSS–1 approximately 6 months, to the fourth quarter of FY 2017. Both have faced similar challenges completing the integration and testing of satellites and ground systems. At the same time, the programs are developing or planning for additional satellites.

Our work on these programs has highlighted the need for effective management to mitigate the potential for gaps in the environmental data provided by NOAA’s current, aging systems. Below we preview the challenges posed by GOES–R, JPSS, and the Polar Follow-On programs, as well as processing data from the GOES–16 and JPSS–1 satellites and new challenges to maintaining satellite coverage.

**Completing and launching GOES–R series satellites.** A number of integration and test problems caused NOAA to delay the GOES–R estimated launch date form March 2016 to October 2016. In addition, a launch anomaly on an international space station resupply mission in March 2016 raised concerns about GOES–R’s launch vehicle. After an investigation and corrective actions, GOES–R’s launch date was postponed from October to November 2016, further threatening NOAA’s ability to maintain a spare, on-orbit satellite. NOAA launched GOES–R on November 19 and renamed it GOES–16. Its on-orbit commissioning has reportedly gone well and once operational, NOAA will have mitigated the risk of a gap in its geostationary satellite coverage.

However, GOES–R development issues and schedule delays have affected the progress of the program’s next mission, GOES–S. NOAA slipped the GOES–S
planned launch date from May 2017 to March 2018. The GOES–R mission’s problems pulled resources away from the GOES–S effort and, in some cases, required the use of GOES–S components as spares for GOES–R. Further, the program is managing a risk related to the need to rework antenna stations, which are on the ground system schedule’s critical path for GOES–S launch readiness.

Completing preparations for the launch of JPSS–1. The JPSS program was committed to launching JPSS–1 no later than the end of the second quarter of FY 2017. However, additional problems with a key instrument and further delays in the completion of its ground system led NOAA and the program to delay the launch, which is now scheduled for September 23, 2017.

The program had to significantly revise the integration and testing sequence of activities for JPSS–1 in order to accommodate the delayed completion of the Advanced Technology Microwave Sounder (ATM) and pivoted support systems (gimbals) for the satellite’s two science mission data antennas. We reported in April 2016 that JPSS–1’s schedule reserves were below the program’s procedural requirements. The satellite’s environmental testing campaign began in mid-March. In July 2016, testing detected additional problems with ATMS that required its removal from the satellite in order to investigate and correct.

The JPSS–1 launch is also contingent upon an upgrade of the JPSS common ground system. This major upgrade will provide new hardware and software, capabilities for supporting JPSS–1, a full backup capability, additional ground antenna stations, multiple operating environments, and significant security improvements. Its completion has been prolonged by software development and integration problems, adding risk to the JPSS–1 launch schedule.

In April 2016—before the discovery of additional problems with ATMS—we concluded that the program’s ability to meet full requirements for JPSS–1 launch was at risk. Further, the program’s need to revise its integration and testing approach to preserve its schedule risked having lower-level system requirements insufficiently tested. In October, NOAA concluded that the instrument and ground system problems presented too much risk to its second quarter launch commitment date and delayed the launch to the fourth quarter.

Recently, the importance of launching JPSS–1 has taken on added urgency. The JPSS program has been responding to more frequent issues with Suomi National Polar-orbiting Partnership (Suomi NPP), which was launched in 2011 and is now operating beyond its designed mission life. Suomi NPP is the only provider of certain JPSS-quality data from the afternoon polar orbit. The loss of that data before JPSS–1 is in operation would result in a data gap that could affect the accuracy of weather forecasts.

Establishing life-cycle cost and schedule baselines for Polar Follow-On program. The JPSS program formulated the acquisition and development of two additional satellites—JPSS–3 and JPSS–4—which are intended to be copies of JPSS–2. Funded under the Polar Follow-On program budget, the missions will be integrated with and managed by the JPSS program. In December 2016, the Deputy Secretary of the Department of Commerce formally approved the Polar Follow-On life-cycle cost and schedule baselines.

Preparing to process observational data from GOES–16 series and JPSS–1. The ground system development problems both programs were addressing risked the deferral of planned operational capabilities until after the launches of GOES–16 and JPSS–1. Management attention to post-launch test activities is needed to ensure users’ needs are met—and to inform a new Administration and Congress of data availability and its effect on forecasts.

The GOES–R program continues to conduct post-launch testing of GOES–16. The results of the testing will indicate whether or not certain planned capabilities will be delayed. For JPSS, we recommended, in our April 2016 report, that the National Weather Service complete a contingency plan to expedite the use of JPSS–1 data, if needed, once the satellite is launched and communicate the plan to users and stakeholders by the end of the third quarter of FY 2016. We also recommended that NOAA provide stakeholders with a list of key activities for operationalizing JPSS–1 data that NOAA will undertake during the poten-

---

11 This referred to schedule reserves toward what was then a January 20, 2017, planned launch date.

tial gap period. However, NOAA has yet to complete these activities in accordance with its audit action plan.

New challenges to maintaining satellite coverage. Issues include the following:

**GOES backup concerns:** NOAA maintains operational geostationary satellites at two positions over the Western Hemisphere: GOES-East (the GOES–13 satellite) and GOES-West (GOES–15). A third satellite (currently, GOES–14) is kept in storage-mode at a location between them and is intended to provide backup capability should either of the operational satellites fail. Events in recent years have demonstrated the need for this redundancy. GOES–13 failures have necessitated a call-up of the backup satellite twice. Additionally, GOES–15 only has one operable star tracker remaining among its three onboard. If the final star tracker fails, GOES–15 will be unable to meet its mission requirements.

**GOES–16,** as the newest and fourth NOAA satellite on orbit, is planned to take one of the operational positions in November 2017.

**JPSS–1 launch delay prolongs potential coverage gap:** NOAA’s need to delay the launch of JPSS–1 from March 2017 to September 2017 prolongs a period of increased risk of a polar satellite coverage gap due to the aging of Suomi NPP beyond its mission design life. In April 2016, using assumptions based on the program status at that time, we had assessed that NOAA would be facing a period of increased risk for 7–10 months starting in November 2016. Now, assuming a JPSS–1 launch in late September 2017, the potential coverage gap period, which began in November 2016, has increased to 14–17 months.

**Ongoing OIG oversight:** Audit of JPSS program performance and Polar Follow-On baseline establishment. For an audit of JPSS and Polar Follow-On programs, our objective is to assess the cost, schedule, and technical performance of selected components of the JPSS program, as well as the establishment of Polar Follow-On program baselines.

**IV. NOAA Fisheries**

**Balancing the priorities of sustainable fisheries with those of multiple stakeholders**

The National Marine Fisheries Service (NOAA Fisheries) must balance two competing interests: (1) promoting commercial and recreational fishing as vital elements of our national economy and (2) preserving populations of fish and other marine life. The Magnuson-Stevens Fishery Conservation and Management Act of 1976 (Magnuson-Stevens Act), gut the Marine Mammal Protection Act of 1972, and the Endangered Species Act of 1973 gave NOAA Fisheries responsibility for rebuilding and maintaining sustainable fisheries and promoting the recovery of protected marine species. The Magnuson-Stevens Act also made NOAA Fisheries the primary Federal agency for managing marine fisheries and established a regional fishery management council system to help the agency carry out its mission.

Developing conservation and management measures requires collecting, analyzing, and reporting demographic information about fish populations via stock assessments. These assessments are a key element of the fishery management process; they are used to determine whether additional regulations are necessary to rebuild fish stocks or whether an increase in fishing opportunities can be allowed. NOAA continues to face challenges to ensuring timely and accurate assessments and providing consultation to its stakeholders. OIG’s oversight of such activity includes responses to members of Congress about regional issues, as well as an upcoming review of NOAA stock assessments.

**Congressional responses:** On June 13, 2016, we received a request from Senators Blumenthal and Murphy and Congressman Courtney asking for information about fishery management across the Northeast and mid-Atlantic. Specifically, they raised issues related to the

- current management structure of black sea bass, summer flounder, and scup, as well as their statutory requirements;
- current structure of fisheries management in the area;
- effectiveness of the quota share transfer between states; and

\(^{13}\) Pub. L. No. 94–265; see also 16 U.S.C. 1801 et seq.
\(^{14}\) Pub. L. No. 92–522; see also 16 U.S.C. 1361 et seq.
\(^{15}\) Pub. L. No. 93–205; see also 16 U.S.C. 1531 et seq.
In its August 30, 2016, response to us, NOAA stated that

- Fisheries released a formal Fisheries Allocation Review Policy and two associated procedural directives to provide a consistent approach for the Councils to periodically re-evaluate fishery allocations.
- NOAA also communicated that the Mid-Atlantic Fisheries Management Council recently voted to increase the New England Fishery Management Council's voting seats on the Demersal Species Committee—under which black sea bass, summer flounder, and scup are managed—to three. In NOAA's estimation, this approach provides another opportunity for Northern states to be involved in the management of these stocks.
- Lastly, NOAA Fisheries is currently considering a request from the New England Fishery Management Council for joint management of black sea bass, summer flounder, and scup.

On September 14, 2016, our Deputy IG's response to the Congressional request stated in part that

- OIG was planning a project to inventory the science that NOAA Fisheries' Office of Science and Technology has used to estimate the population of various fish stocks.
- The Fisheries Management Councils have the authority under the Magnuson-Stevens Act to conduct any activities that are necessary and appropriate to carrying out its functions.
- With respect to issues managing fish stock and quota share transfer, NOAA and the Fisheries Management Councils have the expertise needed to address concerns related to the science used in their decisions.
- OIG presented to NOAA the Congressional concerns raised with respect to issues with the current management structure and liaison model, and requested NOAA to provide a response (which we ultimately included as an enclosure to our response).

In addition, on June 27, 2016, we received a request from Senator Rubio for OIG to review the Department's decisions and assessment modeling, especially the Beaufort Assessment Model, as it relates to the South Atlantic red snapper fishery.

OIG reached out to NOAA for information related to Senator Rubio's request. In its July 27, 2016, response to us, NOAA stated that

- A protracted benchmark stock assessment was conducted for red snapper and gray triggerfish, with various public meetings informing the decisions made with respect to these species, including the use of the Beaufort Assessment Model. This information is consolidated on a public website.
- The decision process related to these species has numerous features involving multiple stakeholders, the South Atlantic Fishery Management Council, and the NOAA Fisheries Southeast Fisheries Science Center, among others.

On August 29, 2016, our Deputy IG replied to the Senator's request by stating in part that

- OIG was planning a project to inventory the science that NOAA Fisheries' Office of Science and Technology has used to estimate the population of various fish stocks.
- OIG conveyed NOAA response to the Senator's concerns.
- To date, we have not encountered or been alerted to specific risks with respect to NOAA's actions or the Fishery Management Council process.

Ongoing OIG oversight: Review of NOAA Fisheries stock assessment enterprise.

NOAA Fisheries manages approximately 500 fish stocks. Its stock assessments examine the effects of fishing and other factors to describe the past and current status of a fish stock, answer questions about the size of a fish stock, and make predictions about how a fish stock will respond to current and future management measures.

On January 13, 2017, OIG initiated a project for inventorying the science that NOAA Fisheries' Office of Science and Technology has used to estimate the population of various fish stocks. NOAA has provided us a list of 40 models and
V. Oversight of the Department’s Management and Spending

IT and cybersecurity issues

Our Cybersecurity Act of 2015 audit identified that the Department faces significant challenges to securing its national security systems. We found that the Department had not followed longstanding requirements for managing the security risks for some of its national security systems. After we disclosed this issue to the Department’s senior management, the Chief Information Officer developed a plan to correct the issues we identified. Currently, the Department is in the process of mitigating the security risks.

The Enterprise Security Operations Center (ESOC) is to provide Department-wide security situational awareness to senior Departmental and bureau managers. To meet OMB’s requirement, the Department has also designated ESOC as its principal security operations center, which will be responsible for coordinating communication with the Department of Homeland Security, U.S. Computer Emergency Readiness Team, and OMB; and sharing cybersecurity intelligence and information with the Department’s bureaus. In August 2016, ESOC began to receive and analyze cybersecurity-related information covering all of the Department’s bureaus.

As part of the Department’s enterprise continuous monitoring initiative, the Enterprise Cybersecurity Monitoring and Operations (ECMO) is to provide timely information about vulnerabilities to system owners in the bureaus. ECMO has been funded through the Department’s working capital fund (WCF). In FY 2016, the Department put the implementation of ECMO on hold until its WCF received additional funding. This action delayed the Department-wide continuous monitoring capabilities to its high-impact systems. Currently, the Department plans to complete the implementation of ECMO on high-impact systems by the end of September 2017.

Creating a Department-wide culture of accountability

Over the course of 2016, OIG’s Office of Investigations (OI) processed more than 500 complaints regarding the Department’s operations; opened more than 80 investigations into allegations of fraud, waste, and abuse related to the Department’s programs and funds; and closed more than 50 open investigations. Many of these closed investigations resulted in successful criminal convictions (8), suspension or debarment actions (10), and administrative disciplinary actions (5).

OI released two investigative reports to the public in 2016. One report described OIG’s detailed analysis of work hours claimed by more than 8,000 patent examiners at the U.S. Patent and Trademark Office. In that investigation, we found hundreds of thousands of hours that examiners claimed to work that could not be supported by evidence of actual work, which equated to more than $18 million in potential waste. The second report detailed evidence gathered by OIG showing how a high-ranking political appointee received multiple unwarranted reimbursements for expenses he incurred during stays at luxury hotel accommodations while on official travel, inappropriately used a subordinate to handle personal tasks for him on a regular basis, and caused his agency to spend thousands of dollars on questionable expenses associated with renovation work that he wanted done to his office suite.

Preventing travel abuse. In the latter case, pertaining to government travel, our inquiries raised concerns about the Department’s compliance with governing laws and rules, particularly the Federal Travel Regulation and the Department’s travel-related policies. In particular, we identified issues with Department personnel involved in the preparation and approval of official travel, specifically with regard to premium-class travel involving senior Department personnel. While some of the problems identified in these inquiries appeared to result from intentional abuse, other failures stemmed from critical misunderstandings of key travel-related laws and rules by one or more employees responsible for administering travel.

NOAA Fisheries’ Alaska Regional Office Use of Contract Raises Issues Regarding Personal Services (Office of Audit and Evaluation product originating from an OI hotline complaint). We reviewed a complaint received in January 2015 from

964 assessments completed since 2004 and their respective scientific models. Our preliminary work is currently underway.
a confidential complainant regarding NOAA Fisheries Alaska Regional Office’s use of grants and cooperative agreements. The objective of our review was to determine whether NOAA inappropriately used a cooperative agreement and grant to acquire personal services, as alleged by the confidential complainant. We were unable to substantiate the complainant’s claim. However, we did find that the regional office used a contract to acquire administrative support services, the execution and management of which contained similarities in appearance to prohibited personal services contracts, which should be avoided to ensure that NOAA Fisheries does not inappropriately supplement its full-time employee workforce.

We recommended the Assistant Administrator for Fisheries (1) develop a control process that restricts future awards from being managed as personal service contracts; and (2) distribute guidance to NOAA Fisheries program staff on statutory restrictions and limitations relating to personal services contracts.

Conference spending issues. On December 2, 2016, we issued a memorandum, Biweekly Reporting on Conference Spending by the Department of Commerce (OIG–17–006–M), that provides the results of OIG’s analysis of biweekly conference spending reports provided by the Department. Our review found the following results:

- **USPTO is likely under-reporting its FY 2016 conference activity to OIG.** In its FY 2015 biweekly submissions to Office of Administration Programs (OAP), the U.S. Patent and Trademark Office (USPTO) reported a total of 36 conferences. In FY 2016, USPTO reported none. OIG noted that USPTO’s interpretation of the policy is overly broad and, through its application, may not be reporting conference information as envisioned by Congress or OMB.

- **It is unclear whether the Census Bureau is under-reporting its FY 2016 conference activity to OIG.** In its FY 2015 biweekly submissions to OAP, the Census Bureau (Bureau) reported a total of 14 conferences. In FY 2016, the Bureau has reported 3. The Bureau’s explanation indicates that, upon clarification of the policy, it stopped reporting these training events. It is not clear who provided this clarification to the Bureau—and, while its explanation refers to an “opinion” to not report on similar events in FY 2016, this opinion was not provided to OIG nor was it described as a legal opinion.

VI. OIG Recommendations Issued to the Department of Commerce

Our office is committed to ensuring that the Department resolves and implements each recommendation provided in our products. Since FY 2015 alone, we have provided 205 recommendations to the Department, identifying program improvements, operational efficiencies, and cost savings in a wide range of programs and activities. For those delivered in FY 2015, 57 of 86 have been implemented by the Department—a rate of 66 percent for those issued during this time. For FY 2016, this rate is currently 30 percent (33 of 111 recommendations implemented), as the Department begins to take action on many of these recommendations in FY 2017. Overall, 115 recommendations—issued between October 1, 2015, and the end of January 2017—remain either unresolved or unimplemented as of the end of January 2017.

Much of our work produces results that directly benefit the taxpayer. With respect to OIG’s return on investment, we have reported more than $125 million in monetary benefits over the last 2 full fiscal years. These include (a) questioned costs and (b) funds to be put to better use as a result of audits and inspections, as well as (c) monetary issues identified by investigations.

In addition to the recent and upcoming work we have highlighted in the above discussion of Department challenges—which included agencies and programs of particular interest to this Committee—OIG is engaged in other oversight work on challenges related to, among other issues,

1. preparations for the 2020 decennial census,
2. U.S. Patent and Trademark Office programs,
3. the National Institute of Standards and Technology,
4. the International Trade Administration’s Commercial Service and Enforcement and Compliance offices, and
5. the Department’s and operating units’ working capital funds and unliquidated obligations.

OIG expresses its appreciation to the former Secretary of Commerce for supporting our efforts as Department management addressed our recommendations. We look forward to the continued support of the incoming Secretary.
This concludes my prepared statement, and I will be pleased to respond to any questions you or other Committee members may have.

The CHAIRMAN. Thank you, Ms. Gustafson.
Mr. Roth?

STATEMENT OF HON. JOHN ROTH, INSPECTOR GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. Roth, Chairman Thune, Ranking Member Nelson, and members of the Committee, thank you for inviting me here to testify today.

As you know, DHS' mission to protect the Nation entails a wide array of responsibilities. Our office reflects the size and complexity of the Department. In a typical year, we issue nearly 200 audit and inspection reports and complete over 600 investigations. In our audit and inspection reports, we make nearly 400 recommendations in an average year. We receive nearly 19,000 complaints through our hotline and website, including hundreds of whistleblower retaliation complaints per year, and have pending nearly 1,000 investigations at any one time.

Although significant progress has been made, the Department continues to face longstanding persistent challenges overseeing and managing its homeland security mission. These challenges affect every aspect of the mission, from preventing terrorism and protecting our border and transportation systems to enforcing our immigration laws, ensuring disaster resiliency, and securing cyberspace. My written testimony talks about each of these issues under the Committee's jurisdiction, but for my oral testimony, I'll simply discuss our work as it relates to TSA.

With regard to TSA's aviation passenger screening responsibilities, we previously identified vulnerabilities in their screening operations caused by a combination of technology failures, insufficient processes, and human error. Fortunately, TSA's response to our finding has represented a marked change from previous practice. TSA's leadership understood the gravity of our findings and moved to revamp training, improve technology, and refine checkpoint policies and procedures in an attempt to increase checkpoint efficiencies. More importantly, the previous administrator reemphasized the security mission of TSA to its work force.

We are in the midst of another round of covert testing of checkpoint operations across the country. We will report our results to this committee as well as other committees of jurisdiction.

While there has been much focus on checkpoint operations, we remain concerned about access to secure areas by airport employees and unauthorized individuals. Controlling access to secured airport areas is critical to the safety of passengers and aircraft for obvious reasons. Unfortunately, the current system has much to be desired. Airport operators are required to perform criminal history and immigration checks prior to granting individuals badges that allow them unescorted access to secure areas, and TSA is required to oversee this process.

Despite TSA's efforts to ensure only cleared individuals enter secure areas, we have identified numerous vulnerabilities. For example, we found that TSA does not have an adequate monitoring process in place to ensure that airport operators properly adjudicated
credential applicants' criminal histories, and we also found weaknesses in the verification process for an individual's authorization to work in the U.S. Weaknesses in this program represent a security risk to aviation transportation.

Moreover, although TSA is required to perform an annual inspection of commercial airport security operations, which includes reviews of the documentation that airport workers had submitted in applying for credentials, we found that at larger airports, TSA looked at as few as 1 percent of all aviation workers' applications. In addition, we found other weaknesses in the method by which the documentation was verified. We have made recommendations to fix these vulnerabilities, and we will follow up to ensure TSA takes the required steps to ensure better performance in this area.

We also have concerns with the sufficiency of vetting itself. Airport workers are subject to only minimal vetting, the same level of vetting, for example, that a pre-check passenger receives, including a fingerprint-based criminal history check to determine whether an individual has been convicted of or is under indictment for certain felonies and whether that person is on the terrorist watch list. The risk presented by such limited vetting is compounded by the fact that airport workers are subject to physical screening at only three of the approximately 450 airports under TSA's jurisdiction. We believe that this creates a significant risk to aviation security.

Additionally, there are significant risks that lost or stolen access badges could allow unauthorized access to secure airport areas. In response to congressional concerns and media reports, we conducted a review of TSA's controls over access badges. Based on its inspections, TSA had asserted to us that most airports adequately control badges for employees working in non-public areas.

However, we found this not to be accurate. TSA had simply relied on the airport operators' assurances that the airports were properly accounting for badges. In fact, in a recent audit where we actually compared employer records against airport records, we found an unacceptable percentage of airport employers had not reported lost or missing badges or failed to recover the badge from those who had left employment. Again, we believe that this represents a significant risk to aviation security.

Mr. Chairman, this concludes my testimony. I'm happy to answer questions you or any members of the Committee may have.

[The prepared statement of Mr. Roth follows:]


Chairman Thune, Ranking Member Nelson, and Members of the Committee, thank you for inviting me to testify on the work of the Office of Inspector General of the Department of Homeland Security.

As you know, DHS' mission to protect the Nation entails a wide array of responsibilities. These range from facilitating the flow of commerce and travelers, countering terrorism, and securing and managing the border to enforcing and administering immigration laws and preparing for and responding to natural disasters.

Our office reflects the size and complexity of the Department. In a typical year, we issue nearly 200 audit and inspection reports and conduct over 600 investigations. In our audit and inspection reports, we make nearly 400 recommendations in an average year. We receive nearly 19,000 complaints through our hotline and website, including over 400 whistleblower complaints per year, and have pending nearly 1,000 investigations at any one time.
Currently, as it relates to matters under this Committee’s jurisdiction, we have 115 open recommendations. A full list of these recommendations is attached as appendix A. The number of open recommendations, particularly those with which the Department did not agree, has fallen precipitously. We are generally pleased with the level of responsiveness we have received from the Department, which we believe is a result of significant leadership commitment to the principles of an independent internal audit function.

**Major Management Challenges Facing DHS**

Homeland Security faces many challenges, and we at OIG have focused our energy on the major management and performance challenges. We have listed six:

- creating a unified department,
- employee morale and engagement,
- acquisition management,
- grants management,
- cybersecurity, and
- improving management fundamentals.\(^1\)

Although significant progress has been made, the Department continues to face long-standing, persistent challenges overseeing and managing its homeland security mission. These challenges affect every aspect of the mission, from preventing terrorism and protecting our borders and transportation systems to enforcing our immigration laws, ensuring disaster resiliency, and securing cyberspace. The Department is continually tested to work as one entity to achieve its complex mission. The key to sustaining the gains made thus far is a leadership commitment by the new Administration and continued thoughtful but vigorous oversight by this Committee and my office.

I will briefly discuss our work in the three areas under the Committee’s jurisdiction: the Transportation Security Administration, the Coast Guard, and the Department’s cyber responsibilities.

**Transportation Security Administration**

*The Nature of the Threat*

Nowhere is the asymmetric threat of terrorism more evident than in the area of aviation security. TSA cannot afford to miss a single, genuine threat without potentially catastrophic consequences, and yet a terrorist only needs to get it right once. Securing the civil aviation transportation system remains a formidable task—with TSA responsible for screening travelers and baggage for over 1.8 million passengers a day at 450 of our Nation’s airports. Complicating this responsibility is the constantly evolving threat by adversaries willing to use any means at their disposal to incite terror.

The dangers TSA must contend with are complex and not within its control. Recent media reports have indicated that some in the U.S. intelligence community warn terrorist groups like the Islamic State (ISIS) may be working to build the capability to carry out mass casualty attacks, a significant departure from—and posing a different type of threat than—simply encouraging lone wolf attacks. According to these media reports, a mass casualty attack has become more likely in part because of a fierce competition with other terrorist networks—being able to kill opponents on a large scale would allow terrorist groups such as ISIS to make a powerful showing. We believe such an act of terrorism would likely be carried out in areas where people are concentrated and vulnerable, such as the Nation’s commercial aviation system.

*Mere Intelligence is Not enough*

In the past, officials from TSA, in testimony to Congress, in speeches to think tanks, and elsewhere, have described TSA as an intelligence-driven organization. According to TSA, it continually assesses intelligence to develop countermeasures in order to enhance the multiple layers of security at airports and onboard aircraft. This is a necessary thing, but it is not sufficient.

In the vast majority of the instances, the identities of those who commit terrorist acts were simply unknown to the intelligence community beforehand. Terrorism, especially suicide terrorism, depends on a cadre of newly-converted individuals who are often unknown to the intelligence community. Moreover, the threat of ISIS- or Al Qaeda-inspired actors—those with no formal ties to the larger organizations, but

---

who simply take inspiration from them—increase the possibilities of a terrorist actor being unknown to the intelligence community.

What this means is that there is no easy substitute for the checkpoint. The checkpoint must necessarily be intelligence driven, but the nature of terrorism today means that each and every passenger must be screened in some way.

TSA Does Not Have a Risk-Based Security Strategy

TSA has many responsibilities beyond air travel, and is responsible, generally through the use of regulation and oversight, for surface transportation security. However, TSA focuses primarily on air transportation security and largely ignores other modes. We found that TSA does not have an intelligence-driven, risk-based security strategy to inform security and budget needs across all types of transportation. In 2011, TSA began publicizing that it uses an “intelligence-driven, risk-based approach” across all transportation modes. However, we found this not to be true. In an audit we released this past September, we reported that TSA specifically designed this approach to replace its one-size-fits-all approach to air passenger screening, but did not apply it to other transportation modes. Additionally, TSA’s agency-wide risk management organizations provide little oversight of TSA’s surface transportation security programs. TSA established an Executive Risk Steering Committee which was intended to create a crosscutting, risk-based strategy that would drive resource allocations across all modes. However, no entity at TSA, places much emphasis on non-air transportation modes.

As a result of a lack of focus on surface transportation, TSA’s efforts in this area have been lacking. Recently, we have published two reports that identify significant weaknesses in TSA’s ability to secure surface transportation modes and the Nation’s maritime facilities and vessels. Specifically, we identified issues with the reliability of background checks for port workers, and passenger rail security.

With regard to surface transportation, we issued a report that found that TSA has failed to develop and implement regulations governing passenger rail security required more than nine years ago. Specifically, although required by the Implementing Recommendations of the 9/11 Commission Act of 2007, TSA neither identified high-risk carriers, nor issued regulations requiring those carriers to conduct vulnerability assessments and implement DHS-approved security plans. TSA also did not issue regulations that would require a railroad security training program. Furthermore, unlike aviation and maritime port workers, TSA has not developed regulations requiring security background checks for rail workers. TSA has just submitted a notice of proposed rulemaking on one rule to the Federal Register, but unfortunately, will not even commit to a timeline as to when they will move the other two regulations forward.

We issued a second report that found that TSA is missing key internal controls in the Transportation Worker Identification Credential (TWIC) program. The background check process for TWICs includes a check for immigration-, criminal-, and terrorism-related offenses that would preclude someone from being granted unescorted access to secure facilities at seaports. Our review found that TSA did not adequately integrate the security measures intended to identify fraudulent applications into the background check process. This was the case notwithstanding the fact that a GAO report found the same problems five years ago.

Checkpoint Performance

Detection of dangerous items on people and in baggage requires reliable equipment with effective technology, as well as well-trained and alert TSOs who understand and consistently follow established procedures and exercise good judgment. We believe there are vulnerabilities in TSA’s screening operations, caused by a combination of technology failures and human error. Since 2004, we have conducted eight covert penetration testing audits on passenger and baggage screening operations. Because these audits involved covert testing and contain classified or Sen-

TSA Penetration Testing of Advanced Imaging Technology (Unclassified Summary), OIG 12–06; Covert Testing of Access Controls to Secured Airport Areas, OIG–12–26; Vulnerabilities Exist in TSA’s Checked Baggage Screening Operations (Unclassified Summary), OIG–14–142.


The results of our covert testing, like the testing we have done in the past, is classified at the Secret level. However, we can describe the results as troubling and disappointing.5

Unfortunately, the results of this covert testing was in line with previous covert testing we had conducted, both on the AIT machines as well as on checked baggage and access to secured airport areas.6

I am pleased to report that in the last 18 months, TSA’s response to our findings has represented a marked change from previous practice. TSA’s leadership understood the gravity of our findings, and moved to revamp training, improve technology, and refine checkpoint policies and procedures in an attempt to increase checkpoint effectiveness. This plan is appropriate because the checkpoint must be considered as a single system; the most effective technology is useless without the right personnel, and the personnel need to be guided by the appropriate procedures. Unless all three elements are operating effectively, the checkpoint will not be effective.

More importantly, the previous Administrator reemphasized the security mission of TSA to the workforce.

We are in the midst of another round of covert testing across the country. Consistent with our obligations under the Inspector General Act, we will report our results to this Committee as well as other committees of jurisdiction.

Expedited Screening and Risk Assessment

We applaud TSA’s efforts to use risk-based passenger screening because it allows TSA to focus on high-risk or unknown passengers instead of known, vetted passengers who pose less risk to aviation security.

However, we have had deep concerns about some of TSA’s previous decisions about this risk. For example, we recently assessed the PreCheck Initiative, which is used at about 125 airports to identify low-risk passengers for expedited airport checkpoint screening. Starting in 2012, TSA massively increased the use of Precheck. Some of the expansion—for example allowing Precheck to other Federal Government-vetted or known flying populations, such as those in the CBP Trusted Traveler Program—made sense. In addition, TSA continues to promote participation in Precheck by passengers who apply, pay a fee, and undergo individualized security threat assessment vetting.

However, we believe that TSA’s use of risk assessment rules, which grant expedited screening to broad categories of individuals based on some questionable assumptions about relative risk based on factors unrelated to individual assessment of risk, create an unacceptable risk to aviation security. We have been communicating with TSA officials about this, and TSA has provided us a plan by which they will decrease reliance on this process. However, we remain concerned about the pace of progress in this area and will continue to monitor the situation.7

Airport Employee Vetting and Access Controls to Secure Areas

Airport employees, as well as unauthorized individuals, entering the secure areas of airports pose a serious potential risk to security. Controlling access to secured areas of commercial airports is critical to the safety of passengers and aircraft. Despite TSA’s efforts to ensure only cleared individuals enter secure areas, we have identified numerous vulnerabilities.

Federal regulations require individuals who apply for credentials to work in secure areas of commercial airports to undergo background checks. TSA and airport operators are required to perform these checks prior to granting individuals badges that allow them unescorted access to secure areas.

We found that TSA was generally effective in identifying individuals with links to terrorism. Since its inception in 2003, TSA has directed airports to deny or revoke 58 airport badges as a result of its vetting process for credential applicants and existing credential holders. In addition, TSA has implemented quality review proc-

---

6 TSA Penetration Testing of Advanced Imaging Technology (Unclassified Summary), OIG 12–06; Covert Testing of Access Controls to Secured Airport Areas, OIG–12–26; Vulnerabilities Exist in TSA’s Checked Baggage Screening Operations (Unclassified Summary), OIG–14–142.
es for its scoring model, and has taken proactive steps based on non-obvious links to identify new terrorism suspects that it nominates to the watchlist.

Despite rigorous processes, TSA did not identify 73 individuals with links to terrorism because TSA is not cleared to receive all terrorism categories under current interagency watchlisting guidance. At our request, the National Counterterrorism Center (NCTC) performed a data match of over 900,000 airport workers with access to secure areas against the NCTC’s Terrorist Identities Datamart Environment (TIDE). As a result of this match, we identified 73 individuals with terrorism-related category codes who also had active credentials. According to TSA officials, the interagency policy in effect at the time prevented the agency from receiving all terrorism-related codes during vetting.

TSA officials recognized that not receiving these codes represents a weakness in its program, and informed us that TSA cannot guarantee that it can consistently identify all questionable individuals without receiving these categories. In response to this audit, the Department worked with the Intelligence Community to ensure that TSA had access to the entire TIDE. This has closed a significant vulnerability, and we are pleased to report that we were able to close our recommendation.

Additionally, this same audit found that TSA also did not have an adequate monitoring process in place to ensure that airport operators properly adjudicated credential applicants’ criminal histories, and also found weaknesses in the verification process for an individual’s authorization to work in the United States. Weaknesses in these programs present a security risk to aviation transportation.

TSA’s Office of Security Operations performed annual inspections of commercial airport security operations, including reviews of the documentation that aviation workers submitted when applying for credentials. However, due to workload at larger airports, this inspection process looked at as few as one percent of all aviation workers’ applications. In addition, we found other weaknesses in the method by which the documentation was verified.

The necessity to permit access to secure areas to only known and trusted individuals should be self-evident. Those with unsupervised, unescorted access to aircraft could secrete dangerous items on board. Unfortunately, the current system has much to be desired. Open source reporting shows that those with unescorted access regularly stow contraband on airplanes. Last week, for example, American Airlines accidentally discovered during routine maintenance 31 pounds of cocaine secreted in the nose of an American Airlines Boeing 757. According to published news reports, this was the second time in three years this had occurred.

Other open source media, as well as congressional hearings, have highlighted the risks involved. In 2015, an avionics technician with unescorted access to airplanes was convicted for his part in a plot to wage violent jihad by driving a bomb-laden van onto the tarmac at the Wichita airport and detonate it. His goal, according to the prosecutors involved in the case, was to inflict maximum casualties just before Christmas. In another instance, a gun-smuggling conspiracy used a baggage handler to smuggle weapons, including loaded weapons, onto flights from Atlanta to New York. Law enforcement authorities were able to confirm that they had shipped approximately 129 firearms in that manner.

Airport workers are subject to only minimal vetting—the same level of vetting, for example, that a PreCheck passenger receives—including a fingerprint-based criminal history check to determine whether an individual has been convicted of or is under indictment for certain enumerated felonies, and whether that person is on the terrorist watch list. The risk presented by such limited vetting is compounded by the fact that airport workers are subject to physical screening at only two of the approximately 450 airports under TSA’s jurisdiction. We believe that this creates a significant risk to aviation security.

Additionally, there is a significant risk that lost or stolen airport access badges could allow unauthorized people access to secure airport areas. In response to congressional concerns and media reports, we conducted a review of TSA’s controls over

---

8 TSA Can Improve Aviation Worker Vetting, OIG–15–98 (June 2015).
12 The felonies are listed at 49 CFR 1542.209.
access badges. Based on its comprehensive and targeted inspections, TSA has asserted that most airports adequately control badges for employees working in non-public areas. However, we found this not to be accurate.

From TSA's own testing conducted in 2015, as well as our own testing recently conducted, we conclude that airports do not always properly account for access media badges after they are issued to employees. TSA's current inspection practice of relying on information reported by airports about access media badges limits its oversight of badge controls. During our inspection, we found that a significant percentage of the airports we looked at did not have accurate information about active access media badges.

By testing more controls, which are designed to curtail the number of unaccounted for badges, TSA could strengthen its oversight of airports. Improved oversight by TSA, including encouraging wider use of airports’ best practices, would help mitigate the risks to airport security posed by unaccounted for employee badges.13

**TSA Business Practices**

We have continuing concerns with TSA’s stewardship of taxpayer dollars spent on aviation security.

Last May, we issued a report on TSA’s Security Technology Integrated Program (STIP), a data management system that connects airport transportation security equipment, such as Explosive Trace Detectors, Explosive Detection Systems, Advanced Technology X-ray, Advanced Imaging Technology, and Credential Authentication Technology. This program enables the remote management of this equipment by connecting it to a centralized server that supports data management, aids threat response, and facilitates equipment maintenance, including automated deployment of software and configuration changes.

However, we found that, while progress has been made, numerous deficiencies continue in STIP information technology security controls, including unpatched software and inadequate contractor oversight. This occurred because TSA typically has not managed STIP equipment in compliance with DHS guidelines regarding sensitive IT systems. Failure to comply with these guidelines increases the risk that baggage screening equipment will not operate as intended, resulting in potential loss of confidentiality, integrity, and availability of TSA’s automated explosive, passenger, and baggage screening programs.

TSA also has not effectively managed STIP servers as IT investments. Based on senior-level TSA guidance, TSA officials did not designate these assets as IT equipment. As such, TSA did not ensure that IT security requirements were included in STIP procurement contracts. This promoted the use of unsupported operating systems that created security concerns and forced TSA to disconnect STIP servers from the network. TSA also did not report all STIP IT costs in its annual budgets, hindering the agency from effectively managing and evaluating the benefits and costs of STIP.14

Another recent audit revealed that the safety of airline passengers and aircraft could be compromised by TSA’s inadequate oversight of its equipment maintenance contracts. TSA has four maintenance contracts valued at about $1.2 billion, which cover both preventive and corrective maintenance for airport screening equipment. Because TSA does not adequately oversee equipment maintenance, it cannot be assured that routine preventive maintenance is performed on thousands of screening units, or that this equipment is repaired as needed, ready for operational use, and operating at its full capacity. In response to our recommendations, TSA agreed to develop, implement, and enforce policies and procedures to ensure its screening equipment is maintained as required and is fully operational while in service.15

**Sensitive Security Information**

I remain concerned about TSA’s use of the Sensitive Security Information (SSI) designation. In our latest report on airport-based IT systems, TSA had demanded the redaction of information that had previously been freely published without objection, and which my IT security experts state poses no threat to aviation security. TSA’s history of abusing the SSI designation is well documented, and we are conducting a review of TSA’s management and use of the SSI designation, which should be out this summer. Inconsistently and inappropriately marking information in our reports as SSI impedes our ability to issue reports to the public that are transparent.

---

13TSA Could Improve Its Oversight of Airport Controls over Access Media Badges, OIG–17–04 (October 2016).
without unduly restricting information, which is key to accomplishing our mission and required under the Inspector General Act.

Coast Guard

Within the Department of Homeland Security, U.S. Customs and Border Protection’s (CBP) Air and Marine Operations (AMO) and the United States Coast Guard (Coast Guard) share responsibility for maritime security missions. At the request of Congress, we reviewed the maritime missions and responsibilities of AMO and the Coast Guard.

We found that the maritime missions and responsibilities of AMO and the Coast Guard are not duplicative. Their efforts to interdict drugs and people bolster the overall effectiveness of DHS’ maritime border security. The agencies contribute to the national strategy of layered maritime security and conduct different activities, which leads to more interdictions. We also found very little overlap in mission locations. For example, of the 206 combined locations where AMO and the Coast Guard conduct operations in customs waters, only 17 of them (8 percent) have similar capabilities and an overlapping area of responsibility.

However, AMO and the Coast Guard could improve coordination and communication at those 17 areas. For example, we found that the majority of those locations did not train together, and nearly half (45 percent) did not coordinate operations or activities.16

We also supervised the annual financial statement audit, which concluded that, as it relates to the internal control environment, the Coast Guard had a number of internal control deficiencies in the areas of financial disclosure reports; accounts receivable; civilian and military payroll; financial reporting process; and accounts payable accrual. However, these deficiencies were not considered significant, and thus were not reported in the agency’s FY 2015 financial statement report.17 The FY 2016 review is ongoing.

With regard to Coast Guard’s information technology issues, however, the financial statement auditors found that there were IT control deficiencies related to access controls, segregation of duties, and configuration management of Coast Guard’s core financial and feeder systems. In many cases, new control deficiencies reflected weaknesses over controls and systems that were new to the scope of the FY 2015 audit. Such deficiencies limited Coast Guard’s ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. These issues, when combined with other IT issues, contributed to a material weakness in IT controls and financial system functionality at the DHS Department-wide level.18

The conclusions reached in that audit are similar to the deficiencies in the Coast Guard IT systems we discovered during our 2015 Federal Information Security Modernization Act (FISMA) audit. For example, we found that the Coast Guard was operating 35 separate information systems without an “Authority to Operate.” This represents 56 percent of Coast Guard’s high-value assets and mission essential systems, and 67 percent of all other systems. A system operating without an authority to operate means the Coast Guard cannot ensure they have implemented effective controls to protect the sensitive information stored and processed by these systems.19 Coast Guard made significant strides in this area between our FY 2015 and FY 2016 FISMA audits, and in our latest review, had reduced the number of systems without an authority to operate to six.20

On a positive note, we conducted a review of the Coast Guard’s major acquisition process. We did so as a result of concerns we had raised in an earlier 2012 audit, which found that the Coast Guard’s schedule-driven acquisition process allowed the construction of Sentinel Class Fast Response Cutter to begin before all of the operational, design and technical risks were resolved. This necessitated modification of the cutters under construction, causing scheduling delays and additional costs. In this verification review, we examined the Coast Guard’s acquisition of a different vessel, the Offshore Patrol Cutter, to see if the Coast Guard had absorbed the lessons from our audit. We found that the Coast Guard’s plans to reduce risks during this acquisition show progress toward achieving the intended results of our earlier

16. AMO and Coast Guard Maritime Missions Are Not Duplicative, But Could Improve with Better Coordination, OIG–17–03 (October 2016).
audit. However, it is too early in the acquisition to determine whether the Coast Guard has fully implemented its plans. We will continue to look at the issue.\textsuperscript{21}

**Cybersecurity Threat Issues**

Our office looked at a number of cyber issues as it relates to DHS in the recent past.

**FISMA**

The Federal Information Security Modernization Act (FISMA) requires Federal agencies to establish security protections for information systems that support their operations and report annually on the effectiveness of information security policies, procedures, and practices. FISMA also requires that the agency OIG perform an annual independent evaluation of the agency’s information security program and practices and report on agency compliance in the following areas:

1. Continuous Monitoring Management
2. Configuration Management
3. Identity and Access Management
4. Incident Response and Reporting
5. Risk Management
6. Security Training
7. Plan of Action and Milestones
8. Remote Access Management
9. Contingency Planning
10. Contractor Systems

Each year the OIG is required to issue two FISMA reports: A general FISMA report concerning the Department’s “Sensitive But Unclassified,” “Secret,” and “Top Secret” systems to the Office of Management and Budget; and a second report based on our assessment of DHS’ intelligence systems to the Intelligence Community Inspector General (IC IG) with no recommendations. Based on the results in our IC IG report, we issue a third report to the Department that includes recommendations for correcting the deficiencies identified regarding DHS’ intelligence systems.

**General FISMA**

For FY 2016, we found that DHS has taken actions to strengthen its information security program.\textsuperscript{22}

On July 22, 2015, in response to cyber-attacks on the Federal Government, the DHS senior leadership ordered DHS and its Components to strengthen their cyber defenses. Components were to implement the following cybersecurity infrastructure measures within 30 days:

- consolidate all of DHS’ Internet traffic behind the Department’s trusted Internet connections,
- implement strong authentication through the use of personal identity verification (PIV) cards for all privileged and unprivileged access accounts,
- achieve 100 percent SA compliance for systems identified by the Component as high value assets and 95 percent compliance for the remaining systems, and
- retire all discontinued operating systems and servers (e.g., Windows XP and Windows Server 2000/2003).

To further enhance the Department’s cyber defense, in January 2016 DHS senior leadership further ordered Components to take the following actions to protect their networks and educate their employees within 45 days:

- establish the capability to perform searches for compromise indicators within 24 hours of detected suspicious network activity,
- remove users’ administrative privileges on workstations connected to the networks, and
- require two-factor authentication for all users accessing the Department’s Homeland Secure Data Network.

The Components have made significant progress in remediating security weaknesses identified, compared to the same period last year. Further, as of May 2016,

\textsuperscript{21} Verification Review of U.S. Coast Guard’s Acquisition of the Sentinel Class-Fast Response Cutter, OIG–12–68.
all Components were reporting information security metrics to the Department, enabling DHS to better evaluate its security posture.

Despite the progress made, Components were not consistently following DHS' policies and procedures to maintain current or complete information on remediating security weaknesses in a timely fashion. Components operated 79 unclassified systems with expired authorities to operate. Further, Components had not consolidated all Internet traffic behind the Department's trusted Internet connections and continued to use unsupported operating systems that may expose DHS data to unnecessary risks. We also identified deficiencies related to configuration management and continuous monitoring. Without addressing these deficiencies, the Department cannot ensure that its systems are adequately secured to protect the sensitive information stored and processed in them.

Intelligence FISMA

Pursuant to FISMA, we reviewed the Department's policies, procedures, and system security controls for the enterprise-wide intelligence system in September of last year. Since our FY 2015 evaluation, the Office of Intelligence and Analysis has continued to provide effective oversight of the department-wide system and has implemented programs to monitor ongoing security practices. In addition, Intelligence and Analysis has relocated its intelligence system to a DHS data center to improve network resiliency and support.

The Coast Guard has migrated all of its sites that process Top Secret/Sensitive Compartmented Information to the Department of Defense Intelligence Information System owned by the Defense Intelligence Agency. However, Coast Guard must continue to work with the Defense Intelligence Agency to clearly identify agency oversight responsibilities for the Department of Defense Intelligence Information System enclaves that support Coast Guard's intelligence operations.23

Science and Technology Directorate Insider Threats

The DHS Science and Technology Directorate (S&T) is the primary DHS research arm. Its mission is to strengthen the Nation's security and resiliency by providing knowledge products and innovative solutions for DHS. Trusted insiders at S&T are given elevated access to mission-critical assets, including personnel, facilities, information, equipment, networks, and systems. Trusted insiders may also be aware of weaknesses in organizational policies and procedures, as well as physical and technical vulnerabilities in computer networks and information systems.

We have begun an audit to assess the effectiveness of steps S&T has taken to protect its IT assets and data from potential unauthorized access, disclosure, or misuse by its employees, contractors, and business partners—especially those with special or elevated access based upon their job descriptions or functions. The scope of our review includes S&T headquarters and selected S&T locations that use or maintain IT systems and data; security operations and incident response centers; and other locations as needed. We expect to complete this performance audit and report on the results in February 2017.

Mr. Chairman, this concludes my testimony. I am happy to answer any questions you or any members of the Committee may have.

<table>
<thead>
<tr>
<th>Report No.</th>
<th>Report Title</th>
<th>Date Issued</th>
<th>Recommendation</th>
<th>Rec. No.</th>
<th>DHS Comp.</th>
<th>Questioned Cost (Federal Share)</th>
<th>Funds to be Put to Better Use (Federal Share)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OIG–15–16 Evaluation of DHS' Information Security Program for Fiscal Year 2014</td>
<td>12/12/2014</td>
<td>We recommend that the Chief Information Security Officer (CISO) evaluate whether the Department's system inventory methodology is effective to prevent Components from circumventing the existing process to procure or develop new systems.</td>
<td>2</td>
<td>MGMT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>OIG–15–16 Evaluation of DHS' Information Security Program for Fiscal Year 2014</td>
<td>12/12/2014</td>
<td>We recommend that the CISO strengthen the process to ensure that all DHS systems receive the proper authority to operate in accordance with applicable OMB and National Institute of Standards and Technology (NIST) security authorization guidance.</td>
<td>6</td>
<td>MGMT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>OIG–16–08 Evaluation of DHS' Information Security Program for Fiscal Year 2015</td>
<td>11/13/2015</td>
<td>We recommend that the DHS CISO strengthen the Department’s oversight of the Component’s information security programs to ensure they comply with requirements throughout the year instead of peaking in compliance during the months leading up to annual Federal Information Security Management Act of 2002, as amended (FISMA) reporting.</td>
<td>3</td>
<td>MGMT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>OIG–16–08 Evaluation of DHS' Information Security Program for Fiscal Year 2015</td>
<td>11/13/2015</td>
<td>We recommend that DHS CISO implement input validation controls on DHS' enterprise management systems and perform quality reviews to validate that the information entered is accurate.</td>
<td>5</td>
<td>MGMT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>OIG–12–26 Transportation Security Administration Covert Testing of Access Controls to Secured Airport Areas</td>
<td>1/6/2012</td>
<td>This is a classified report.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>OIG–14–132 Audit of Security Controls for DHS Information Technology Systems at Dallas' Fort Worth International Airport</td>
<td>9/5/2014</td>
<td>We recommend that the TSA Chief Information Officer (CIO) establish a process to report Security Technology Integrated Program (STIP) computer security incidents to TSA Security Operations Center (SOC).</td>
<td>3</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>OIG–14–132</td>
<td>Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport</td>
<td>9/5/2014</td>
<td>We recommend that the TSA Chief Information Officer (CIO) provide required vulnerability assessment reports to the DHS Vulnerability Management Branch.</td>
<td>5</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>------------</td>
<td>---------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>---</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>OIG–14–142</td>
<td>(U) Vulnerabilities Exist in TSA’s Checked Baggage Screening Operations</td>
<td>9/16/2014</td>
<td>This is a classified report.</td>
<td>4</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>OIG–14–142</td>
<td>(U) Vulnerabilities Exist in TSA’s Checked Baggage Screening Operations</td>
<td>9/16/2014</td>
<td>This is a classified report.</td>
<td>5</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>OIG–15–18</td>
<td>Audit of Security Controls for DHS Information Technology Systems at John F. Kennedy International Airport-Sensitive Security Information</td>
<td>12/16/2014</td>
<td>We recommend that the TSA CIO designate the intrusion detection and surveillance Security Systems as DHS information technology (IT) systems and implement applicable management, technical, operational, and privacy controls and reviews.</td>
<td>6</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>OIG–15–29</td>
<td>Security Enhancements Needed to the TSA PreCheck™ Initiative</td>
<td>1/28/2015</td>
<td>This recommendations contains Sensitive Security Information.</td>
<td>1</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>OIG–15–29</td>
<td>Security Enhancements Needed to the TSA PreCheck™ Initiative</td>
<td>1/28/2015</td>
<td>This recommendations contains Sensitive Security Information.</td>
<td>2</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>OIG–15–29</td>
<td>Security Enhancements Needed to the TSA PreCheck™ Initiative</td>
<td>1/28/2015</td>
<td>This recommendations contains Sensitive Security Information.</td>
<td>4</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>OIG–15–29</td>
<td>Security Enhancements Needed to the TSA PreCheck™ Initiative</td>
<td>1/28/2015</td>
<td>This recommendations contains Sensitive Security Information.</td>
<td>5</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>OIG–15–29</td>
<td>Security Enhancements Needed to the TSA PreCheck™ Initiative</td>
<td>1/28/2015</td>
<td>This recommendations contains Sensitive Security Information.</td>
<td>9</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>Report No.</td>
<td>Report Title</td>
<td>Date Issued</td>
<td>Recommendation</td>
<td>Rec. No.</td>
<td>DHS Comp.</td>
<td>Questioned Cost (Federal Share)</td>
<td>Funds to be Put to Better Use (Federal Share)</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
<td>---------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>17</td>
<td>OIG–15–29 Security Enhancements Needed to the TSA PreCheck™ Initiative</td>
<td>1/28/2015</td>
<td>We recommend that the TSA Assistant Administrator for the Office of Intelligence and Analysis: Employ exclusion factors to refer TSA PreCheck® passengers to standard security lane screening at random intervals.</td>
<td>10</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>OIG–15–29 Security Enhancements Needed to the TSA PreCheck™ Initiative</td>
<td>1/28/2015</td>
<td>We recommend that the TSA Assistant Administrator for the Office of Security Operations: Develop and implement a strategy to address the TSA PreCheck® lane covert testing results.</td>
<td>13</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>OIG–15–29 Security Enhancements Needed to the TSA PreCheck™ Initiative</td>
<td>1/28/2015</td>
<td>(SSI) This recommendation contains Sensitive Security Information.</td>
<td>14</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>OIG–15–45 Allegations of Granting Expedited Screening through TSA PreCheck Improperly (OSC File No. HI–14–3679)</td>
<td>3/16/2015</td>
<td>(SSI) This recommendation contains Sensitive Security Information.</td>
<td>1</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>OIG–15–86 The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program</td>
<td>5/6/2015</td>
<td>We recommend that TSA's Office of Security Capabilities and Office of Security Operations develop and implement a preventive maintenance validation process to verify that required routine maintenance activities are completed according to contractual requirements and manufacturers' specifications. These procedures should also include instruction for appropriate TSA airport personnel on documenting the performance of Level 1 preventive maintenance actions.</td>
<td>1</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>OIG–15–86 The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program</td>
<td>5/6/2015</td>
<td>We recommend that TSA's Office of Security Capabilities and Office of Security Operations Develop and implement policies and procedures to ensure that local TSA airport personnel verify and document contractors' completion of corrective maintenance actions. These procedures should also include quality assurance steps that would ensure the integrity of the information collected.</td>
<td>2</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We recommend that the TSA CIO provide required vulnerability assessment reports to the DHS Vulnerability Management Branch for STIP servers tested, similar to those operating at San Francisco International Airport (SFO).

We recommend that the TSA CIO update the operating systems on STIP servers to a vendor-supported version that can be patched to address emerging vulnerabilities.

We recommend that the TSA Acting Administrator implement all necessary data quality checks necessary to ensure that all credential application data elements required by TSA Security Directive 1542-04-08G are complete and accurate.

We recommend that the Assistant Administrator, Office of Human Capital for TSA and the Federal Air Marshal Service conduct a cost-benefit analysis to ensure all costs are considered to implement one medical case management system for TSA, including its Federal Air Marshal Service.

We recommend that TSA’s Assistant Administrator for the Office of Acquisition ensure that Personnel Futures Program (PFP) contracts contain lessons learned from the human capital services (HHS) contract that include—developing and implementing policy guidance for administering award fee type contracts;—monetary penalties for performance deficiencies including violating Federal law;—performance timeframes and prescriptive language in the statement of works (SOW);—performance metrics that correspond to the majority of sections in the SOWs;—timeframes for correcting performance deficiencies; and—requirements for initiating and issuing performance letters, and for factoring performance deficiencies addressed in those letters into performance evaluations and award determinations.
<table>
<thead>
<tr>
<th>Report No.</th>
<th>Report Title</th>
<th>Date Issued</th>
<th>Recommendation</th>
<th>Rec. No.</th>
<th>DHS Comp</th>
<th>Questioned Cost (Federal Share)</th>
<th>Funds to be Put to Better Use (Federal Share)</th>
</tr>
</thead>
<tbody>
<tr>
<td>28 OIG–16–87</td>
<td>IT Management Challenges Continue in TSA’s Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that IT security controls are included in STIP system design and implementation so that STIP servers are not deployed with known technical vulnerabilities.</td>
<td>1</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29 OIG–16–87</td>
<td>IT Management Challenges Continue in TSA’s Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that STIP servers use approved operating systems for which the Department has established minimum security baseline configuration guidance.</td>
<td>2</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30 OIG–16–87</td>
<td>IT Management Challenges Continue in TSA’s Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that STIP servers have the latest software patches installed so that identified vulnerabilities will not be exploited.</td>
<td>3</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31 OIG–16–87</td>
<td>IT Management Challenges Continue in TSA’s Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that IT security testing is performed so that STIP servers are not deployed with known technical vulnerabilities.</td>
<td>4</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32 OIG–16–87</td>
<td>IT Management Challenges Continue in TSA’s Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that authorized TSA staff obtain and change administrator passwords for all STIP servers at airports so that contractors no longer have full control over this equipment at airports.</td>
<td>5</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33 OIG–16–87</td>
<td>IT Management Challenges Continue in TSA’s Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly implement a contractor oversight process so that only authorized and approved software, along with timely updates, is installed on STIP airport servers.</td>
<td>6</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>OIG–16–87</td>
<td>IT Management Challenges Continue in TSA's Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly inventory all locations at Orlando International Airport housing STIP servers and switches and ensure that these locations comply with DHS policy concerning physical security controls.</td>
<td>7</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>OIG–16–87</td>
<td>IT Management Challenges Continue in TSA's Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure an adequate operational recovery capability for STIP servers at Data Center 1 (DC1) in case Data Center 2 (DC2) becomes inaccessible.</td>
<td>8</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>OIG–16–87</td>
<td>IT Management Challenges Continue in TSA's Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly establish a process for providing STIP server vulnerability assessment reports to the Department so that DHS leadership may adequately monitor system compliance capability.</td>
<td>9</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>OIG–16–87</td>
<td>IT Management Challenges Continue in TSA's Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly ensure that IT security requirements are included in equipment procurement contracts for IT components of STIP and passenger and checked baggage screening equipment as required.</td>
<td>10</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>OIG–16–87</td>
<td>IT Management Challenges Continue in TSA's Security Technology Integrated Program</td>
<td>5/10/2016</td>
<td>We recommend that the TSA CIO and Assistant Administrator for OSC jointly institute controls so that all IT costs associated with STIP are accurately captured and reported in annual budget submissions as required.</td>
<td>11</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>OIG–16–91</td>
<td>TSA Oversight of National Passenger Rail System Security</td>
<td>5/13/2016</td>
<td>We recommend that the TSA Administrator ensure TSA develops and adheres to a detailed, formal milestone plan to deliver the remaining 9/11 Act Notices of Proposed Rulemaking to DHS.</td>
<td>1</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>OIG–16–128</td>
<td>TWIC Background Checks are Not as Reliable as They Could Be</td>
<td>9/1/2016</td>
<td>We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration conduct a comprehensive risk analysis of the Security Threat Assessment processes to identify areas needing additional internal controls and quality assurance procedures, and develop and implement those procedures, including periodic reviews to evaluate their effectiveness.</td>
<td>2</td>
<td>TSA</td>
<td></td>
</tr>
<tr>
<td>Report No.</td>
<td>Report Title</td>
<td>Date Issued</td>
<td>Recommendation</td>
<td>Rec. No.</td>
<td>DHS Comp</td>
<td>Questioned Cost (Federal Share)</td>
<td>Funds to be Put to Better Use (Federal Share)</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>41</td>
<td>OIG–16–128 TWIC Background Checks are Not as Reliable as They Could Be</td>
<td>9/1/2016</td>
<td>We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration improve Transportation Worker Identification Credential program-level performance metrics to ensure they align with the program’s core objectives, and direct management officials to use these metrics for all the supporting offices.</td>
<td>3</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>OIG–16–128 TWIC Background Checks are Not as Reliable as They Could Be</td>
<td>9/1/2016</td>
<td>We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration review current Transportation Worker Identification Credential Security Threat Assessment guidance to ensure it provides adjudicators the necessary information and authority to complete Security Threat Assessments.</td>
<td>4</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>OIG–16–134 TSA Needs a Crosscutting Risk-Based Security Strategy</td>
<td>9/9/2016</td>
<td>We recommend that the Deputy Administrator, TSA, develop and implement a crosscutting risk-based security strategy that encompasses all transportation modes. The strategy should, at a minimum:—define intelligence-driven, risk-based security;—identify objectives for an intelligence-driven, risk-based security approach;—identify steps for all transportation modes to achieve risk-based security objectives;—provide guidelines for aligning resources with risk;—establish priorities, milestones, and performance measures to gauge the effectiveness of the strategy; and—establish responsible parties and timelines for strategy implementation.</td>
<td>1</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>OIG–16–134 TSA Needs a Crosscutting Risk-Based Security Strategy</td>
<td>9/9/2016</td>
<td>We recommend that the Deputy Administrator, TSA, establish a formal budget planning process that uses risk to help inform resource allocations.</td>
<td>3</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>OIG–17–04 TSA Could Improve Its Oversight of Airport Controls over Access Media Badges</td>
<td>10/14/2016</td>
<td>We recommend that the TSA Administrator: Direct TSA personnel to conduct additional tests of access media badge controls during comprehensive and targeted inspections of U.S. airports.</td>
<td>1</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIG–17–04</td>
<td>TSA Could Improve Its Oversight of Airport Controls over Access Media Badges</td>
<td>10/14/2016</td>
<td>We recommend that the TSA Administrator: Issue guidance to U.S. airports clearly explaining how to determine whether an airport’s lost, stolen, and unaccounted for access media badges are exceeding the 5 percent threshold.</td>
<td>2</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIG–17–04</td>
<td>TSA Could Improve Its Oversight of Airport Controls over Access Media Badges</td>
<td>10/14/2016</td>
<td>We recommend that TSA share with airport operators the best practices some airports use to mitigate the risks of lost, stolen, and unaccounted for access media badges and encourage airport operators to use these practices when feasible.</td>
<td>3</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIG–17–14</td>
<td>Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports</td>
<td>11/29/2016</td>
<td>We recommend that the TSA CIO update TSA’s Business Impact Analyses for TSA Network (TSANet) and Security Technology Integrated Program (STIP) to include the TSA local area networks (LAN) points of contact, and business processes that would be adversely affected by a potential communications outage at airports.</td>
<td>1</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIG–17–14</td>
<td>Summary Report on Audits of Security Controls for TSA Information Technology Systems at Airports</td>
<td>11/29/2016</td>
<td>We recommend that the TSA CIO establish a plan to conduct recurring reviews of the operational, technical, and management security controls for TSA IT systems at U.S. airports nationwide.</td>
<td>2</td>
<td>TSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIG–10–11</td>
<td>Independent Auditors’ Report on DHS’ FY 2009 Financial Statements and Internal Control Over Financial Reporting</td>
<td>11/13/2009</td>
<td>We recommend that the Coast Guard design and implement policies, procedures, and internal controls to support the completeness, existence, accuracy, and presentation and disclosure assertions related to the data utilized in developing disclosure and related supplementary information for Stewardship property, plant, and equipment (PP&amp;E) that is consistent with generally accepted accounting principles (GAAP).</td>
<td>I–D.8</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report No.</td>
<td>Report Title</td>
<td>Date Issued</td>
<td>Recommendation</td>
<td>Rec. No</td>
<td>DHS Core</td>
<td>Questioned Cost (Federal Share)</td>
<td>Funds to be Put to Better Use (Federal Share)</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------</td>
<td>-------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>52</td>
<td>OIG–11–86 U.S. Coast Guard’s Marine Safety Program—Offshore Vessel Inspections</td>
<td>6/1/2011</td>
<td>We recommend that the Assistant Commandant for Marine Safety, Security and Stewardship, U.S. Coast Guard complete and disseminate to field units New Construction Project Inspector Performance Qualification Standards and update the Marine Safety Manual accordingly.</td>
<td>1 USCG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>OIG–11–86 U.S. Coast Guard’s Marine Safety Program—Offshore Vessel Inspections</td>
<td>6/1/2011</td>
<td>We recommend that the Assistant Commandant for Marine Safety, Security and Stewardship, U.S. Coast Guard augment Marine Information for Safety and Law Enforcement (MISLE) access controls, and develop subsequent policy, so that the same person cannot open, complete, and close an inspection case.</td>
<td>3 USCG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>OIG–12–07 Independent Auditors’ Report on DHS FY 2011 Integrated Financial Statements and Internal Control over Financial Reporting</td>
<td>11/11/2011</td>
<td>We recommend that the Coast Guard, establish new or improve existing policies, procedures, and related internal controls to ensure that: The year-end close-out process, reconciliations, and financial data and account analysis procedures are supported by documentation, including evidence of effective management review and approval, and beginning balances in the following year are determined to be reliable and auditable.</td>
<td>IA.3.a</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>OIG–12–07 Independent Auditors’ Report on DHS FY 2011 Integrated Financial Statements and Internal Control over Financial Reporting</td>
<td>11/11/2011</td>
<td>We recommend that the Coast Guard, establish new or improve existing policies, procedures, and related internal controls to ensure that: All intra-governmental activities and balances are reconciled on a timely basis, accurately reflected in the financial statements, and differences are resolved in a timely manner in coordination with the Department’s Office of Financial Management (OFM).</td>
<td>IA.3.e</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>OIG–13–20 Independent Auditors’ Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting</td>
<td>11/14/2012</td>
<td>We recommend that the Coast Guard establish new or improve existing policies, procedures, and related internal controls to ensure that: All non-standard adjustments (i.e., journal entries, top-side adjustments, and scripts) impacting the general ledger are adequately researched, supported, and reviewed prior to their recording in the general ledger.</td>
<td>IA.1.c.i</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>OIG–13–20</td>
<td>Report Title</td>
<td>Date</td>
<td>Recommendation</td>
<td>I.A.1.c.ii</td>
<td>USCG</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>-----------</td>
<td>--------------</td>
<td>------</td>
<td>---------------</td>
<td>-----------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>Independent Auditors’ Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting</td>
<td>11/14/2012</td>
<td>We recommend that the Coast Guard establish new or improve existing policies, procedures, and related internal controls to ensure that: All non-GAAP policies are identified and their quantitative and qualitative financial statement impacts have been documented.</td>
<td>I.A.1.c.ii</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>Independent Auditors’ Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting</td>
<td>11/14/2012</td>
<td>We recommend that the Coast Guard: Continue to improve the enforcement of existing policies and procedures related to processing obligation transactions and the periodic review and validation of undelivered orders. In particular, emphasize the importance of performing effective reviews of open obligations, obtaining proper approvals, and retaining supporting documentation.</td>
<td>I.E.1.a</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>Independent Auditors’ Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting</td>
<td>11/14/2012</td>
<td>We recommend that the Coast Guard: Continue with current remediation efforts to develop and implement policies, procedures, and internal controls over the monitoring of reimbursable agreements and unfilled customer orders to ensure activity, including closeout and de-obligation, is recorded timely and accurately.</td>
<td>I.E.1.b</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Independent Auditors’ Report on DHS FY 2012 Consolidated Financial Statements and Report on Internal Control Over Financial Reporting</td>
<td>11/14/2012</td>
<td>We recommend that the Coast Guard: Implement sufficient policies and procedures for recording the appropriate budgetary entries timely upon receipt of goods, and prior to payment.</td>
<td>I.E.1.c</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>Identification, Reutilization, and Disposal of Excess Personal Property by the United States Coast Guard</td>
<td>12/21/2012</td>
<td>We recommend that the Assistant Commandant for Resources and Chief Financial Officer (CFO) develop and implement a demilitarization program, in coordination with the Department of Defense Demilitarization Office, that includes training and certification for United States Coast Guard personnel who manage, oversee, or process personal property from acquisition to disposal.</td>
<td>3</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report No.</td>
<td>Report Title</td>
<td>Date Issued</td>
<td>Recommendation</td>
<td>Rec. No.</td>
<td>DHS Comp.</td>
<td>Questioned Cost (Federal Share)</td>
<td>Funds to be Put to Better Use (Federal Share)</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>62</td>
<td>OIG–13–19 Identification, Reutilization, and Disposal of Excess Personal Property by the United States Coast Guard</td>
<td>12/21/2012</td>
<td>We recommend that the Assistant Commandant for Resources and CFO develop and implement a process to enter and track all classified personal property in the Oracle Fixed Asset Module. Develop and implement standardized policies and procedures to ensure accountability, monitoring, and oversight of disposal of classified personal property components (e.g., hard drives and printer cartridges).</td>
<td>4</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>OIG–13–19 Identification, Reutilization, and Disposal of Excess Personal Property by the United States Coast Guard</td>
<td>12/21/2012</td>
<td>We recommend that the Assistant Commandant for Resources and CFO develop and implement a comprehensive training program, to include reutilization and disposal, for property managers, tailored to each level of personal property management responsibility. The training should include Commanding Officers, Accountable Property Officers, Personal Property Administrators, and Property Custodians and mandatory training for Oracle Fixed Asset Module users before granting future access.</td>
<td>6</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>OIG–13–19 Identification, Reutilization, and Disposal of Excess Personal Property by the United States Coast Guard</td>
<td>12/21/2012</td>
<td>We recommend that the Assistant Commandant for Resources and CFO develop and implement policies and procedures to account for newly purchased computers that comply with the U.S. Coast Guard's Personal Property Management Manual requirement for entry of personal property into the Oracle Fixed Asset Module within 30 calendar days of receipt from the vendor.</td>
<td>7</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>OIG–13–92 Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard</td>
<td>5/23/2013</td>
<td>We recommend that the USCG Assistant Commandant for Resources and CFO implement an investigations and inspections retention plan to ensure qualified personnel are retained within the inspections and investigations specialties.</td>
<td>1</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Report Type</td>
<td>Document Title</td>
<td>Date</td>
<td>Recommendation</td>
<td>Source</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------</td>
<td>------</td>
<td>----------------</td>
<td>--------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>OIG–13–92</td>
<td>Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard</td>
<td>5/23/2013</td>
<td>We recommend that the USCG Assistant Commandant for Resources and CFO revise and strengthen its personnel management policies by implementing provisions of the 2010 Coast Guard Authorization Act, which allows promotions by specialty for marine inspectors and investigators to foster retention and continuity.</td>
<td>2</td>
<td>USCG</td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>OIG–13–92</td>
<td>Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard</td>
<td>5/23/2013</td>
<td>We recommend that the USCG Assistant Commandant for Resources and CFO develop a complete process with sufficient resources to review, track, and address all recommendations resulting from investigations reports.</td>
<td>3</td>
<td>USCG</td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>OIG–13–92</td>
<td>Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard</td>
<td>5/23/2013</td>
<td>We recommend that the USCG Assistant Commandant for Resources and CFO provide training and guidance to all investigations personnel on all enforcement options.</td>
<td>5</td>
<td>USCG</td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>OIG–13–92</td>
<td>Marine Accident Reporting, Investigations, and Enforcement in the United States Coast Guard</td>
<td>5/23/2013</td>
<td>We recommend that the USCG Assistant Commandant for Resources and CFO provide enforcement training guidelines for preparing and supporting Civil Penalty cases for all investigations staff. USCG should consider using officers with previous experience in the Hearing Office to complete this task.</td>
<td>6</td>
<td>USCG</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>OIG–14–18</td>
<td>Independent Auditors' Report on DHS' FY 2013 Financial Statements and Internal Control over Financial Reporting</td>
<td>12/11/2013</td>
<td>We recommend that Coast Guard: Fully adhere to established inventory policies and procedures.</td>
<td>C.1b</td>
<td>USCG</td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>OIG–14–18</td>
<td>Independent Auditors' Report on DHS' FY 2013 Financial Statements and Internal Control over Financial Reporting</td>
<td>12/11/2013</td>
<td>We recommend that Coast Guard: Establish new or improve existing processes to identify and evaluate lease agreements to ensure that they are appropriately classified as operating or capital, and are properly reported in the financial statements and related disclosures.</td>
<td>C.1.d</td>
<td>USCG</td>
<td></td>
</tr>
<tr>
<td>Report No.</td>
<td>Report Title</td>
<td>Date Issued</td>
<td>Recommendation</td>
<td>Rec. No.</td>
<td>DHS Comp.</td>
<td>Questioned Cost (Federal Share)</td>
<td>Funds to be Put to Better Use (Federal Share)</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-------------</td>
<td>----------------</td>
<td>----------</td>
<td>-----------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>72 OIG–15–10</td>
<td>Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2014</td>
<td>We recommend that Coast Guard: Adopt policies, procedures, and accounting treatments documented in ad hoc technical accounting research papers into official financial reporting guidance that is distributed agency wide; and refine financial reporting policies and procedures to prescribe process level internal controls at a sufficient level of detail to ensure consistent application to mitigate related financial statement risks.</td>
<td>1.a.b</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>73 OIG–15–10</td>
<td>Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2014</td>
<td>We recommend that Coast Guard: Identify and employ additional skilled resources.</td>
<td>1.a.c</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>74 OIG–15–10</td>
<td>Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2014</td>
<td>We recommend that Coast Guard, establish new or improve existing policies, procedures, and related internal controls to ensure that: Environmental liability schedules are updated, maintained, and reviewed.</td>
<td>1.a.i</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>75 OIG–15–10</td>
<td>Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2014</td>
<td>We recommend that Coast Guard, establish new or improve existing policies, procedures, and related internal controls to ensure that: Underlying data used in the estimation of environmental liabilities is complete and accurate.</td>
<td>1.a.ii</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>76 OIG–15–10</td>
<td>Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2014</td>
<td>We recommend that Coast Guard, establish new or improve existing policies, procedures, and related internal controls to ensure that: Accrual decisions and/or calculations as well as the validation of prior year accrual amounts are properly reviewed.</td>
<td>1.a.iii</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>77 OIG–15–10</td>
<td>Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2014</td>
<td>We recommend that Coast Guard: Design and implement controls to appropriately track asset activity at a transaction level and ensure the timely recording of asset additions, deletions, or other adjustments.</td>
<td>1.C.1 a</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Report ID</td>
<td>Report Title</td>
<td>Issue Date</td>
<td>Recommendation</td>
<td>Agency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-----------</td>
<td>--------------</td>
<td>------------</td>
<td>----------------</td>
<td>--------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>OIG–15–10</td>
<td>Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2014</td>
<td>We recommend that Coast Guard: Continue to implement controls over the transfer of completed construction in progress assets to in-use and accurately recording leasehold improvements, asset impairments, and construction in progress activity.</td>
<td>1.C.1.b USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>OIG–15–10</td>
<td>Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2014</td>
<td>We recommend that Coast Guard: establish new or improve existing policies, procedures, and related internal controls to sufficiently support personal and real property balances, including electronics, internal-use software, land, buildings and other structures.</td>
<td>1.C.1.d USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>OIG–15–10</td>
<td>Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2014</td>
<td>We recommend that Coast Guard: establish new, or improve existing, processes to identify and evaluate lease agreements to ensure they are appropriately classified as operating or capital, and are properly reported in the financial statements and related disclosures.</td>
<td>1.C.1.e USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>OIG–15–10</td>
<td>Independent Auditors' Report on DHS' FY 2014 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2014</td>
<td>We recommend that Coast Guard: Identify and employ additional skilled resources.</td>
<td>1.C.1.f USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>OIG–15–55</td>
<td>United States Coast Guard Has Taken Steps to Address Insider Threats, but Challenges Remain</td>
<td>3/27/2015</td>
<td>We recommend that the USCG CIO: Implement software to protect against the unauthorized removal of sensitive information through removable media devices and e-mail accounts.</td>
<td>1 USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>OIG–15–55</td>
<td>United States Coast Guard Has Taken Steps to Address Insider Threats, but Challenges Remain</td>
<td>3/27/2015</td>
<td>We recommend that the USCG CIO: Implement stronger physical security controls to protect USCG's IT assets from possible loss, theft, destruction, and malicious actions.</td>
<td>2 USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>OIG–16–06</td>
<td>Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/13/2015</td>
<td>We recommend that Coast Guard: Establish new, or improve existing, policies, procedures, and related internal controls.</td>
<td>1.a USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report No.</td>
<td>Report Title</td>
<td>Date Issued</td>
<td>Recommendation</td>
<td>Rec. No.</td>
<td>DHS Comp.</td>
<td>Questioned Cost (Federal Share)</td>
<td>Funds to be Put to Better Use (Federal Share)</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----------</td>
<td>-------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>85</td>
<td>Independent Auditors’ Report on DHS’ FY 2015 Financial Statements and</td>
<td>11/13/2015</td>
<td>We recommend that Coast Guard establish new or improve existing policies, procedures, and related internal controls to ensure that: Transactions flowing between various general ledger systems, whether the result of remediation or system limitation manual workarounds, are sufficiently tracked and analyzed to ensure complete and accurate reporting of operational activity and related general ledger account balances.</td>
<td>1.a ii</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal Control over Financial Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>Independent Auditors’ Report on DHS’ FY 2015 Financial Statements and</td>
<td>11/13/2015</td>
<td>We recommend that Coast Guard: Establish new or improve existing policies, procedures, and related internal controls to ensure: The year-end close-out process, reconciliations, and financial data and account analysis procedures are supported by documentation, including evidence of effective management review and approval; and beginning balances in the following year are determined to be reliable and supported.</td>
<td>1.a v</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal Control over Financial Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>Independent Auditors’ Report on DHS’ FY 2015 Financial Statements and</td>
<td>11/13/2015</td>
<td>We recommend that Coast Guard establish new or improve existing policies, procedures, and related internal controls to ensure that: All intragovernmental activities and balances are reconciled on a timely basis, accurately reflected in the financial statements, and differences are resolved in a timely manner.</td>
<td>1.a vi</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal Control over Financial Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>Independent Auditors’ Report on DHS’ FY 2015 Financial Statements and</td>
<td>11/13/2015</td>
<td>We recommend that Coast Guard establish new or improve existing policies, procedures, and related internal controls to ensure that: Adequate understanding and oversight of assumptions used in significant estimates is maintained by Coast Guard management and continued appropriateness of those assumptions are routinely evaluated.</td>
<td>1.a vii</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal Control over Financial Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>Independent Auditors’ Report on DHS’ FY 2015 Financial Statements and</td>
<td>11/13/2015</td>
<td>We recommend that Coast Guard: Identify and employ additional skilled resources and align them to financial reporting oversight roles.</td>
<td>1.c</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal Control over Financial Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Page</td>
<td>Section</td>
<td>Recommendation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>----------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>1.C.1.b</td>
<td>Develop processes and monitoring mechanisms to track construction-in-progress (CIP) projects at an asset level and continue to implement management controls to improve the accuracy of CIP costs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>1.C.1.c</td>
<td>Design contracts for Coast Guard’s major construction projects to isolate costs between development and maintenance (i.e., capitalizable vs. expense), at an individual asset level, in order to enhance traceability of CIP costs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>1.C.1.e</td>
<td>Establish new or improve existing policies, procedures, and related internal controls to sufficiently review personal and real property, to include operations, equipment, vessels, and other structures, and verify costs are appropriate and reflect USCG’s business operations during the fiscal year.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>94</td>
<td>1.C.1.f</td>
<td>Establish new, or improve existing, processes to identify and evaluate lease agreements to ensure they are appropriately classified as operating or capital, and are properly reported in the financial statements and related disclosures.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>1.C.1.h</td>
<td>Develop and implement procedures to support the completeness, accuracy, and existence of all data utilized in the financial statements and related disclosures.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report No.</td>
<td>Report Title</td>
<td>Date Issued</td>
<td>Recommendation</td>
<td>Rec. No.</td>
<td>DHS Comp</td>
<td>Questioned Cost (Federal Share)</td>
<td>Funds to be Put to Better Use (Federal Share)</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>-------------</td>
<td>----------------</td>
<td>----------</td>
<td>----------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>96</td>
<td>OIG–16–06 Independent Auditors' Report on DHS FY 2015 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/13/2015</td>
<td>We recommend that Coast Guard: Develop a comprehensive understanding of their actuarial evaluations and document the sources of all underlying data and assumptions.</td>
<td>1.e</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>OIG–16–15 (U) Fiscal Year 2015 Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems</td>
<td>12/14/2015</td>
<td>This recommendation is classified.</td>
<td>2</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>OIG–16–15 (U) Fiscal Year 2015 Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems</td>
<td>12/14/2015</td>
<td>This recommendation is classified.</td>
<td>3</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>99</td>
<td>OIG–16–15 (U) Fiscal Year 2015 Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems</td>
<td>12/14/2015</td>
<td>This recommendation is classified.</td>
<td>4</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>OIG–17–12 Independent Auditors' Report on DHS FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2016</td>
<td>We recommend that DHS develop continuous monitoring and testing of IT general controls to identify weaknesses, assess the resulting risks created by any identified IT deficiencies, and respond to those risks through implementing compensating controls.</td>
<td>2</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Date</td>
<td>Title</td>
<td>Recommendation</td>
<td>Page</td>
<td>Agency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>--------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>11/14/2016</td>
<td>Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to ensure that transactions flowing between various general ledger systems, whether the result of balance clean-up activities or system limitation manual workarounds, are sufficiently tracked and analyzed to ensure complete and accurate reporting of operational activity and related general ledger account balances.</td>
<td>5</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>11/14/2016</td>
<td>Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to ensure that all non-standard adjustments (i.e., journal entries and top side adjustments) impacting the general ledger are adequately researched, supported, and reviewed prior to their recording in the general ledger.</td>
<td>6</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>103</td>
<td>11/14/2016</td>
<td>Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to ensure that the year-end close-out process, reconciliations, and financial data and account analysis procedures are supported by documentation, including evidence of effective management review and approval, and beginning balances in the following year are determined to be reliable and supported.</td>
<td>7</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>11/14/2016</td>
<td>Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to ensure that all intra-governmental activities and balances are reconciled, accurately reflected in the financial statements, and differences are resolved in a timely manner.</td>
<td>8</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>11/14/2016</td>
<td>Independent Auditors' Report on DHS' FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to ensure that Management possesses adequate understanding, maintains documentation, exercises oversight of chosen assumptions, and routinely evaluates the completeness and accuracy of underlying data and the continued appropriateness of assumptions used in significant estimates.</td>
<td>9</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report No.</td>
<td>Report Title</td>
<td>Date Issued</td>
<td>Recommendation</td>
<td>Rec. No</td>
<td>DHS Comp</td>
<td>Questioned Cost (Federal Share)</td>
<td>Funds to be Put to Better Use (Federal Share)</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------</td>
<td>---------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>106</td>
<td>Independent Auditors' Report on DHS FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2016</td>
<td>We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to increase training and development of existing resources to better align them to financial reporting oversight roles.</td>
<td>10</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>Independent Auditors' Report on DHS FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2016</td>
<td>We recommend that Coast Guard design and implement controls to appropriately track asset activity at the transaction level and ensure the timely recording of asset additions, deletions, or other adjustments.</td>
<td>19</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>Independent Auditors' Report on DHS FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2016</td>
<td>We recommend that Coast Guard develop processes and monitoring mechanisms to track CIP projects at an asset level, continue to implement controls over the transfer of completed CIP to in-use assets, and increase monitoring of CIP activity to ensure accurate recording in the general ledger.</td>
<td>20</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>Independent Auditors' Report on DHS FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2016</td>
<td>We recommend that Coast Guard involve financial management personnel in the procurement of contracts for Coast Guard's major construction projects to ensure that they are structured to facilitate isolation of costs between development and maintenance (i.e., capitalizable vs. expensed), at an individual asset level, in order to enhance traceability of CIP costs.</td>
<td>21</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>Independent Auditors' Report on DHS FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2016</td>
<td>We recommend that Coast Guard adhere to established inventory policies and procedures.</td>
<td>22</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>111</td>
<td>Independent Auditors' Report on DHS FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2016</td>
<td>We recommend that Coast Guard establish new, or improve existing, policies, procedures, and related internal controls to sufficiently review personal and real property activity and balances in order to verify costs are appropriate and reflect USCG's business operations during the fiscal year.</td>
<td>23</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIG-17-12</td>
<td>Independent Auditors’ Report on DHS’ FY 2016 Financial Statements and Internal Control over Financial Reporting</td>
<td>11/14/2016</td>
<td>We recommend that Coast Guard attract and deploy additional skilled resources to support the control environment and provide the necessary financial reporting oversight.</td>
<td>24</td>
<td>USCG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIG-17-03</td>
<td>AMO and Coast Guard Maritime Missions Are Not Duplicative, But Could Improve with Better Coordination</td>
<td>10/14/2016</td>
<td>We recommend that the Coast Guard Commandant, CBP Commissioner, and U.S. Immigration and Customs Enforcement Director revise the Maritime Operations Coordination Plan to include requirements for coordination and information sharing at all levels, especially the local level.</td>
<td>2</td>
<td>USCG, CBP, ICE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIG-16-105</td>
<td>DHS’ Use of Reimbursable Work Agreements with GSA</td>
<td>6/23/2016</td>
<td>We recommend that the DHS Under Secretary for Management ensure that deobligation has occurred for the following two reimbursable work agreements that the component was unable to prove had been done.—Coast Guard Reimbursable Work Agreements (RWA) #N3288960—$43,575 should be deobligated—Coast Guard RWA #B0511609—$2,779,654 should be deobligated.</td>
<td>3</td>
<td>USCG, MGMT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIG-16-105</td>
<td>DHS’ Use of Reimbursable Work Agreements with GSA</td>
<td>6/23/2016</td>
<td>We recommend that the DHS Under Secretary for Management conduct a review of the following three reconciliation differences for the reimbursable work agreements, determine the reasons for the differences, and make any necessary corrections.—Coast Guard RWA #N3288960—$12,328,407 expenditure difference—Coast Guard RWA #B0511609—$320,228 expenditure difference—USCIS RWA #N3322206—$45,500 expenditure difference.</td>
<td>2</td>
<td>USCIS, USCG, MGMT</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Monetary Findings $12,694,185 $2,823,229

Total Recommendations as of December 31, 2016: 115
The CHAIRMAN. Thank you, Mr. Roth.
Mr. Scovel?

STATEMENT OF HON. CALVIN L. SCOVEL III, INSPECTOR GENERAL, U.S. DEPARTMENT OF TRANSPORTATION

Mr. ScoVel, Chairman Thune, Ranking Member Nelson, members of the Committee, thank you for inviting me to testify on DOT's top management challenges and unimplemented recommendations. I greatly appreciate the Committee's sustained keen interest and your support for Offices of Inspector General, including mine. It's an honor to be here today with several fellow IGs whose well respected work is critical to the management of our country's resources, safety, and security.

Every year, my office reports on significant challenges for DOT. My testimony today focuses on three critical areas we identified for DOT for 2017: safety, stewardship, and completion of mandates and recommendations.

As Secretary Chao stated clearly during her confirmation hearing, safety remains at the forefront of DOT's mission.

The United States continues to have one of the safest transportation systems in the world. However, new technologies and industries bring new challenges. For example, FAA recently issued a rule to help safely integrate small unmanned aircraft systems, known as UAS, into our airspace. However, the number of UAS sightings by pilots and others continues to go up. Over 1,400 were reported for the first three quarters of 2016, as compared to only 238 in all of 2014. Many of these occurred at altitudes well above the 400 feet maximum altitude authorized by FAA for civil UAS. Maintaining safety will require a strong, risk-based oversight system by FAA and coordination with other agencies.

DOT and NHTSA face similar safety challenges with driverless car technology. Several companies are already developing and testing various iterations, and the number is expected to grow quickly. DOT and policymakers must clearly define the tools and standards necessary to oversee and regulate this industry and the technology underlying it.

At the same time, NHTSA must continue to improve its processes for investigating vehicle safety defects. Most recently, a Takata airbag defect resulted in 11 fatalities and 180 injuries. Due in part to my office's investigative work, Takata Corporation has recalled tens of millions of vehicles and agreed last month to pay $1 billion in criminal penalties. NHTSA is making progress toward addressing our recommendations to collect and analyze more comprehensive vehicle safety data, but must continue to improve internal controls within its Office of Defects Investigations.

With regard to stewardship, we have identified areas where DOT can improve how it manages and oversees the billions of dollars invested each year in our transportation infrastructure. For example, FAA faces ongoing challenges to deliver six programs that are essential to implement NextGen and modernize our outdated air traffic control systems. Cost estimates for these programs now total over $5.7 billion, and their completion has been pushed beyond 2020. As a watch item, many requirements remain undefined, and
FAA has yet to fully quantify how these programs will achieve expected benefits for the aviation industry.

Protecting our infrastructure also requires addressing increasingly sophisticated cybersecurity threats. However, DOT has not effectively implemented programs to actively monitor and mitigate security breaches immediately during or after an incident. Recent trends in mobile, cloud, and workplace technology also present new challenges to monitoring and securing DOT’s network.

Finally, as it carries out its mission, DOT must develop strategies to efficiently carry out mandated and recommended improvements. These include provisions in the 2015 FAST Act to improve investments in highway and transit projects as well as key aviation safety mandates from the 2016 FAA Extension Act. The FAA mandates include, for example, requiring better records on a pilot’s training and background. DOT has also faced delays in addressing recommendations to improve pipeline and hazardous material safety issued by both our office and NTSB.

In conclusion, my office will continue to assist DOT and Congress as we work to meet these and other challenges, including helping the Department leverage its resources to promote safety and efficiency and prevent fraud in any forthcoming infrastructure investment plans. We will also continue to keep you informed as to the status of specific recommendations we have made to the Department.

Mr. Chairman, this concludes my prepared statement. I’m happy to answer any questions you or other committee members may have.

The prepared statement of Mr. Scovel follows:

PREPARED STATEMENT OF HON. CALVIN L. SCOVEL III, INSPECTOR GENERAL, U.S. DEPARTMENT OF TRANSPORTATION

TOP MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF TRANSPORTATION

Chairman Thune, Ranking Member Nelson, and Members of the Committee:

Thank you for inviting me here today to discuss the Department of Transportation’s (DOT) top management challenges. Safe, efficient, and innovative transportation is critical to the U.S. and global economy and essential to creating opportunities that enhance our quality of life. Every year, the Department invests more than $70 billion in a wide range of programs to protect and modernize our transportation infrastructure. Our office supports these efforts through our audits1 and criminal investigations, which promote effectiveness and root out fraud, waste, and abuse in Federal programs. We look forward to working with our Secretary and this Committee to help uphold DOT’s commitment to the traveling public. We report annually to the Administration and Congress on DOT’s top management challenges. My statement today will focus on the challenges2 our work has identified along three cross-cutting areas: (1) addressing new and ongoing safety challenges, (2) enhancing stewardship of DOT’s financial and growing infrastructure investments, and (3) effectively addressing existing mandates and recommendations.

Summary

As Secretary of Transportation Elaine L. Chao has affirmed, DOT’s primary objective is safety. Meeting this objective requires addressing a number of new and ongoing challenges—from ensuring the safe integration of emerging technologies such as Unmanned Aircraft Systems (UAS) and driverless cars to promptly investigating

1 For a list of our ongoing audits, see the exhibit.

2 Top Management Challenges for Fiscal Year 2017, Department of Transportation (OIG Report No. PT2017007), November 15, 2016. OIG reports and testimonies are available on our website: https://www.oig.dot.gov.
Addressing New and Ongoing Safety Challenges

Safety remains the Department’s highest priority, and DOT is committed to improving how it oversees our Nation’s airspace, roads, pipelines, and other critical systems. Yet, emerging technologies, industry safety concerns, and enforcement issues pose challenges to DOT’s safety mission. Key focus areas we have identified for DOT include ensuring its oversight keeps pace with the rapid rise of UAS and driverless cars, improving how it collects and uses vehicle safety recall data, and effectively addressing pipeline safety violations.

Overseeing an Expanding and Dynamic Unmanned Aircraft Systems Industry

Through a sustained focus, DOT, the Federal Aviation Administration (FAA), and industry have maintained a safe aviation system, with no fatal passenger accidents involving domestic commercial carriers in over 7 years. However, the growing demand for commercial UAS operations—for purposes ranging from pipeline monitoring and precision agriculture to package delivery and filmmaking—presents one of the most significant safety challenges for FAA in decades. FAA recently forecast 1.9 million units in potential annual sales of UAS in 2016, which could increase to 4.3 million units sold annually by 2020. While this represents substantial opportunities for U.S. businesses, it also raises safety concerns, since FAA has not yet established a comprehensive oversight framework to ensure this evolving industry can operate safely in the same airspace with other private, commercial, and military aircraft.

FAA took an important step forward to advance UAS integration in June 2016 with a new rule regulating the use of small UAS (i.e., systems weighing less than 55 pounds). However, the rule does not yet permit several high-profile aspects of potential UAS use, such as delivering packages beyond the line of sight of the pilot, underscoring the need for further regulatory efforts. Until then, FAA will continue to accommodate some UAS operations through regulatory waivers and exemptions.

Moreover, as the number of UAS operations has grown, so has the number of UAS sightings by pilots and other sources. In 2015, there were over 1,100 UAS events reported compared to just 238 in 2014, according to FAA’s UAS event data. As shown in the figure below, 71 percent of sightings occurred at altitudes at or above the 400-feet maximum FAA-authorized altitude for civil UAS—with 29 percent of sightings reported at altitudes at or above 3,000 feet, approaching areas where other aircraft operate.

---

3 14 CFR Part 107 (June 2016).
4 While sightings are primarily reported by pilots, reports also come from air traffic controllers, law enforcement officers, and the general public.
5 It is important to note that FAA has not verified the validity of the reports received by air traffic, but the data indicate that a number of UAS operators may be flying their aircraft outside of FAA guidelines.
These events highlight the importance of establishing a risk-based system for UAS oversight, especially since the number of UAS sightings has continued to increase—with over 1,400 reported for the 9-month period ending in September 2016, according to FAA. However, FAA’s efforts in this area are incomplete. For example, the Agency lacks a robust data reporting and tracking system for UAS activity. It also has provided only limited UAS-related training and guidance to safety inspectors. As a result, FAA is currently restricted to a reactive approach for addressing UAS incidents and issues as they arise, rather than proactively identifying and mitigating potential risks.

As we recently reported, to make progress FAA will need to establish the capacity for integrated UAS data and analysis and implement a process to verify UAS operators’ compliance with regulations. Further, FAA must continue coordinating with other Government agencies to advance UAS detection technology. These steps are critical to ensure that FAA can meet UAS demand while maintaining the safety of the NAS.

Preparing To Oversee Driverless Cars

The emergence of driverless cars is another developing technology that will present significant regulatory and oversight challenges for DOT. While this is still in the early stages, several companies are already developing and testing driverless cars, and the number is expected to grow quickly over the next decade. In September 2016, DOT issued a Federal Automated Vehicles Policy, which sets the framework for the next 50 years with guidance for the safe and rapid development of advanced automated vehicle safety technologies. Along with developing the tools and standards to oversee and regulate this new technology, DOT will need to consider the impact on several of its agencies and work to ensure they can adapt as needed to maintain DOT’s commitment to both safety and innovation. For example, the National Highway Traffic Safety Administration (NHTSA) will have to consider whether new authority is needed to ensure that these new vehicles are as safe as standard motor vehicles. Similarly, for commercial motor vehicles, the Federal Motor Carrier Safety Administration (FMCSA) needs to identify any impact to its safety regulations and update operational procedures as required.

Enhancing Processes for Collecting and Analyzing Vehicle Safety Recall Data

Recent large-scale recalls from auto manufacturers highlight a number of safety challenges for the Department. Since 2014, General Motors (GM) has recalled nearly 9 million U.S. vehicles for a defect involving a faulty ignition switch that resulted in GM receiving more than 100 death claims and more than 200 injury claims. In addition, NHTSA is overseeing a recall of Takata airbags installed in tens of millions of U.S. vehicles due to a safety defect that led to 11 fatalities and approximately 180 injuries in the United States. Due in part to our investigative work,
Takata Corporation agreed last month to pay a total of $1 billion in criminal penalties.

NHTSA's Office of Defects Investigation (ODI) is responsible for overseeing safety recalls and monitoring recall completion rates. The GM and Takata recalls and others have prompted congressional concerns over NHTSA's safety processes. We have issued numerous audit recommendations over the years to the Agency to strengthen its internal controls and use of safety data. NHTSA is working to address those concerns, but more work remains. For example, NHTSA recently completed work on 12 of the 17 recommendations from our 2015 audit, which found ODI had insufficient processes for verifying that manufacturers submit complete and accurate early warning reporting data. However, NHTSA has not completed our five recommendations to enhance collection and analysis of early warning reporting data and the process for reviewing complaints. We also reported in February 2016 that ODI needed better quality control mechanisms to comply with policies that NHTSA established in response to our 2011 recommendations involving documentation and testing weaknesses. Those two recommendations from our 2016 report remain open.

This month, we plan to announce an audit of ODI's recall processes as mandated by Congress in the Fixing America's Surface Transportation Act (FAST Act). Consistent with this mandate, and as agreed to with congressional staff, our audit will examine NHTSA's processes for monitoring manufacturers' proposed recall remedies and scope and overseeing safety recall implementation. We will keep Congress apprised of our progress in this area.

Addressing Violations of Pipeline Safety Regulations

A key DOT mission is mitigating the safety risks posed by the Nation's 2.5 million-mile pipeline transportation system. The Pipeline and Hazardous Materials Safety Administration (PHMSA) develops and enforces regulations for the safe and reliable operation of pipelines. However, PHMSA has faced challenges enforcing some key regulatory safeguards. There have been a number of serious pipeline-related incidents over the past several years. From 2012 to 2016, there were 144 serious pipeline incidents resulting in 63 fatalities. Many of these were due to violations of safety regulations required by the Natural Gas Pipeline Safety Act (PSA).

Historically, however, it has been difficult to prosecute such violations due to language in Title 49 U.S.C. Section 60123(a), the criminal statute for pipeline safety violations. This section requires that the violation be committed "knowingly and willfully." Instead, the Department of Justice has had more success prosecuting cases under Section 5124 (the criminal statute for hazardous materials violations), which allows prosecutions for "reckless" violations (i.e., display of deliberate indifference or conscious disregard to the consequences of their conduct). In the past 10 years, Federal charges under Section 60123(a) were brought against only four individuals and companies, and in only one case did a prosecution result in a guilty verdict of a utility company for violations of Section 60123(a)—the case against the Pacific Gas and Electric Company (PG&E).

The case against PG&E arose after a natural gas pipeline ruptured in San Bruno, CA, in 2010, killing 8 people. It was investigated by the Department of Justice, our office, the Federal Bureau of Investigation, and local law enforcement. On August 9, 2016, a federal jury found PG&E guilty of multiple knowing and willful violations of the Federal Transportation Safety Board's (NTSB) investigation. On January 26, 2017, the maximum sentence was imposed—5 years of probation and a $3 million fine. The court also ordered the company to announce in local and national media that it was found guilty of violating the PSA and obstructing a Federal investigation. While this sentence sends a message to the industry, as a policy matter, DOT and Congress may wish to consider whether the deterrent effect of prosecuting violations of the PSA might be enhanced by amending Section 60123(a) to include reckless violations.

Enhancing Stewardship of DOT's Financial and Infrastructure Investments

DOT receives billions of Federal dollars annually to fund projects to build, repair, and maintain our Nation's vast transportation infrastructure, ranging from air traf-
fic control tools to roads and bridges and IT systems. Safeguarding these and future investments requires sound financial management and strong upfront risk mitigation strategies for increasing threats. Key challenges for the Department include enhancing the capacity and resiliency of the NAS, increasing oversight of high-risk contracts and Departmentwide financial programs, and effectively addressing rapidly evolving cybersecurity risks.

**Enhancing the Capacity, Efficiency, and Resiliency of the NAS**

FAA operates the safest aviation system in the world and continues to work with stakeholders to implement new technologies that are providing near-term benefits to airspace users, such as fuel savings and increased airspace capacity and efficiency. However, FAA faces ongoing challenges with its investments to deliver specific capabilities and programs required to implement the Next Generation Air Transportation System (NextGen), which aims to modernize and replace 1950s-era ground radar and equipment.

For example, FAA has worked with industry to identify and begin implementing the four highest priority NextGen capabilities: (1) advancing performance-based navigation (PBN), (2) improving access to closely spaced parallel runways, (3) enhancing airport surface operations, and (4) developing data communications for controllers and pilots. However, FAA is behind schedule in key areas and faces challenges achieving the full range of benefits, particularly with its top priority to develop new PBN procedures. These have faced delays due in part to community concerns over aircraft noise and the lack of automated tools to help controllers sequence and space aircraft.

We also recently reported that FAA has not fully identified the total costs, capabilities, or completion schedules for any of the six NextGen transformational programs that are required to implement NextGen and introduce key capabilities. Cost estimates for these six programs now total over $5.7 billion (increasing from a $2.1 billion estimate in 2012), and their completion has been pushed beyond 2020. Many of these programs’ benefits remain unquantified as to how they will improve the flow of air traffic or controller workforce productivity. For example, FAA has mandated that all airspace users must purchase and install the Automatic Dependent Surveillance-Broadcast System (ADS–B) equipment by 2020. However, the majority of benefits are expected from ADS–B In, which will enable display of information in the cockpit. Yet, ADS–B In’s requirements and associated schedule and costs continue to evolve, making it uncertain when benefits from enhancing NAS capacity will be achieved.

While working to increase capacity and efficiency through NextGen, FAA must also take steps to ensure that the NAS can quickly recover from catastrophic—sometimes intentional—events. For example, in September 2014, an FAA contract employee deliberately started a fire at FAA’s Chicago Air Route Traffic Control Center that disrupted air traffic for more than 2 weeks and led to reported industry losses of over $350 million. The event highlighted weaknesses in FAA’s current air traffic control infrastructure, which has limited flexibility to respond to system failures and quickly return to normal operations. We recently reported that while FAA has begun to develop new contingency plans to better respond to such failures, the plans are still incomplete, and many of the key technologies, such as the new NAS Voice System, are years away from implementation.

**Increasing Oversight of High-Risk Contracts**

DOT relies on billions of dollars in contracts each year to fund programs across all modes of transportation. In Fiscal Years 2015 and 2016, DOT spent over $6 billion in contracts annually. Our work has identified areas where the Department can improve its internal controls and accountability in managing its sizable investments, including strengthening oversight and planning for contracts and minimizing the use of contract types that present the greatest financial risks to the Government.

---


13 The six transformational programs are Automatic Dependent Surveillance-Broadcast (ADS–B), System Wide Information Management (SWIM), Data Communications (DataComm), NAS Voice System (NVS), Common Support Services-Weather (CSS-Wx), and Collaborative Air Traffic Management–Technologies (CATM–T).

14 ADS–B Out involves the broadcast of information to FAA ground systems.

15 Although FAA Has Taken Steps To Improve its Operational Contingency Plans, Significant Work Remains To Mitigate Effects of Major System Disruptions, (OIG Report No. AV2017020) January 11, 2017.

16 NAS Voice System (NVS) is expected to standardize the voice communication infrastructure among FAA air traffic facilities by replacing 11 aging analog voice communication systems with a single digital technology.
For example, cost-reimbursable contracts are considered high risk because of the potential for cost escalation and the fact that the Government pays a contractor’s costs of performance regardless of whether the work is completed. Our review of six Operating Administrations found that they did not (1) perform adequate acquisition planning and document their justifications for using this contract type or (2) consistently assess oversight risks, properly designate oversight personnel, or verify that contractors’ accounting systems are adequate to provide reliable cost data.

Similarly, we found that FAA—which awards more contract dollars annually than any other Operating Administration—lacked basic internal controls and contracting practices for its sole-source and multiple-award contracts. Sole-source contracts are negotiated without the benefit of competition and carry the risk of overspending. Our work found that FAA did not do enough to reduce its use of sole-source contracts, as directed by OMB in 2009. Between Fiscal Years 2008 and 2014, FAA awarded 624 sole-source contracts with a total value of about $2.2 billion. For most of the sole-source contracts we reviewed, FAA had not conducted an adequate market analysis or developed independent cost estimates to ensure reasonable prices. We also found issues with FAA multiple-award service contracts. While multiple award service contracts are not by nature high-risk, the various task orders issued under them frequently lack sufficient oversight and competition. For example, for FAA’s $1.1 billion Systems Engineering 2020 (SE–2020) contracts, FAA did not ensure full competition or documentation for task orders or ensure contract oversight had the needed skills for their jobs. This can increase the risk of cost overruns or payment for services that do not meet DOT’s needs.

Improving Stewardship of Credit Programs and Managing Delinquent Debt

To be an effective steward of taxpayer dollars while financing large infrastructure projects, DOT must carefully manage the consolidation of credit programs that leverage private investment, such as the Transportation Infrastructure Finance and Innovation Act (TIFIA) and the Railroad Rehabilitation and Improvement Financing (RRIF). In 2014, DOT established the Build America Transportation Investment Center (BATIC) to streamline public-private coordination when planning and implementing infrastructure projects. Since BATIC’s inception, DOT credit programs have issued credit instruments totaling roughly $10 billion to 21 projects that support up to $26 billion in transportation infrastructure. Recognizing BATIC’s impact on funding for infrastructure projects, Congress mandated the restructuring of DOT credit programs to consolidate the TIFIA and RRIF programs with BATIC in 2015. This restructuring is ongoing; sustained management attention will be critical to complete and oversee these significant financial arrangements.

Managing DOT’s financial commitments also includes establishing and maintaining internal controls to more effectively identify and collect delinquent debt. Our audit work found that weak internal controls at DOT contributed to an increase in outstanding debt owed the Federal Government by individuals and non-Federal entities and an increased risk that these debts would not be collected and returned to DOT. From Fiscal Years 1999 to 2013, DOT’s reported delinquent debt increased by over 300 percent, from approximately $170 million to $737 million. DOT-wide policies and procedures are needed to accurately identify and report delinquent debt.
and recoveries, collect debts in a timely manner, and ensure DOT has the requisite skills and internal controls for carrying out these programs.

**Coordinating Technological Initiatives and Extending Security Boundaries to Address Cybersecurity Risks**

As cybersecurity threats become increasingly sophisticated and more numerous, DOT faces the challenge of reevaluating and expanding traditional approaches to secure IT systems. DOT must work to fulfill existing requirements while also implementing new strategies to meet the additional security demands of mobile technology, cloud-based computing, and other technological developments. However, cybersecurity remains a significant challenge for DOT and its Operating Administrations.

To its credit, DOT has supplied personal identification verification (PIV) cards to all its employees. However, DOT has not fully implemented the use of these cards Departmentwide for access to its facilities and information systems. In fact, only 140 of its 460 systems (30 percent) can use PIV cards for access. In addition, 530 FAA facilities do not use PIV cards for physical access. DOT also has not effectively implemented other cybersecurity initiatives, such as programs to actively monitor and mitigate security weaknesses immediately during or after an attack. For example, we recently reported that DOT's continuous monitoring program lacks sufficient maturity to be effective, leaving the Department's systems vulnerable to exploitable hardware and software.

Furthermore, recent trends in mobile, cloud, and workplace technology—such as the proliferation of smartphones and tablets and an increasing number of remote employees—present new challenges to monitoring and securing DOT's network. As the industry moves towards extending desktop virtualization and cloud computing, DOT will need to change how it stores and manages data in order to effectively respond to cybersecurity incidents. As we recently reported, DOT's current incident monitoring is incomplete due to lack of access to FAA's and cloud service providers' systems.

**Effectively Addressing Existing Mandates and Recommendations**

In recent years, DOT has faced a significant challenge to implement mandated and recommended improvements to its safety oversight and program management. These include MAP–21 provisions for highway and transit projects, issued in 2012, as well as 2015 FAST Act requirements. In 2016, the FAA Extension, Safety, and Security Act (Extension Act) also set out new requirements for DOT regarding pilot safety issues and oversight of foreign repair stations. At the same time, DOT has struggled to meet deadlines for mandates and recommendations regarding pipeline and hazardous materials safety. Going forward, it will be important for DOT to prioritize actions to meet statutory requirements, weigh rulemakings will have the greatest safety merit and which existing regulations may require additional scrutiny, and assess steps needed to meet these or any future congressional directives. For example, DOT will need to improve its compliance with the Federal Information Technology Acquisition Reform Act (FITARA), which is intended to improve agencies' IT acquisitions and enhance congressional monitoring. DOT recently received a failing grade on the House Committee on Oversight and Government Reform's FITARA Scorecard.

**Implementing Legislative Requirements for Highway and Transit Projects**

MAP–21 established requirements for States to employ performance-based management of DOT's highway and transit programs, including linking State transportation performance plans to Federal-aid highway funds through an asset management plan. As DOT finalizes rulemakings to meet these requirements, it will need to adjust its risk-based oversight to ensure that States consistently comply with the new rules and that the rules achieve desired outcomes. Additionally, MAP–21 called for DOT to accelerate highway, bridge, and transit project delivery. These actions include rulemakings to streamline the environmental review process and required

---


27 For example, the Federal Highway Administration (FHWA) has established a process for development of a State risk-based asset management plan, including defining minimum standards for developing and operating bridge and pavement management systems, and a rulemaking for setting performance targets and measures covering bridges and pavement.
reports to Congress on environmental actions. DOT has implemented half of the actions it initially identified. However, DOT recognizes that it needs to revise a large number of its planned actions to comply with more recent FAST Act requirements that will affect these areas. This includes, for example, a rulemaking that allows States to assume FHWA responsibilities under the National Environmental Policy Act for environmental reviews, consultation, and compliance for Federal highway projects.

Managing New Safety Requirements From the FAA Extension Act

FAA has several ongoing initiatives to enhance aviation safety but faces challenges to implement new requirements of the 2016 Extension Act. Several of the act’s provisions also mirror recommendations from our office. For example, in line with our recent report,29 the act includes requirements for new pilot training on monitoring flight automation systems and new inspector guidance for tracking and assessing pilot proficiency in manual flight. FAA will need to ensure that air carrier training programs address these provisions so that pilots maintain the skills needed to fly safely and recover from a failure with cockpit automated systems or an unexpected event, particularly in the critical phases of flight.

A critical safety component reflected in the Extension Act is ensuring air carriers have the information they need on a pilot’s training and background to make informed hiring decisions. We have monitored FAA’s efforts to establish a pilot records database since it was first mandated in 2010. We reported in 201529 that FAA’s progress has been limited; currently, FAA does not expect to complete the database by the act’s deadline of April 2017. In response, FAA accelerated efforts to launch its portion of the database and expects it to be available to air carriers this month. However, FAA has yet to decide how best to obtain and input air carrier records as far back as 2005, as the act requires, given the differences among carriers’ data and recordkeeping systems. FAA is working on a rulemaking to address this problem and expects to issue it in 2018, at the earliest.

Another aviation safety priority that we have reported on since 2003 is foreign repair stations. Currently there are approximately 840 repair stations located outside the United States. Under the Extension Act, FAA must ensure that its safety assessment system prioritizes inspections at foreign repair stations performing heavy maintenance for U.S. carriers, using risk-based oversight and data to track corrective actions. However, we continue to find weaknesses in FAA’s ability to get the data it needs to assess risk and effectively monitor foreign repair stations covered under the United States and European Union (EU) Aviation Safety Agreement, which went into effect in 2011 and covers more than 400 FAA-certificated repair stations in Europe.31 Currently, foreign authorities are only required to provide FAA with repair station inspection results pertaining to those FAA regulations that differ from the EU’s—not complete facility inspection reports. In response to our recommendation in 2015,32 FAA is developing procedures to obtain these facility inspection reports, which should help it to better assess risk.

Addressing Pipeline and Hazardous Materials Safety Recommendations and Mandates

Given the number of pipeline and hazardous materials incidents over the last several years—more than 86,000 incidents between 2012 and 2016—PHMSA has received many mandates and recommendations to improve how it mitigates these safety risks. Specifically, since 2005, PHMSA has received 263 mandates and recommendations. To its credit, PHMSA completed nearly two-thirds of them but in doing so, missed about 75 percent of its mandated deadlines. Our work shows that PHMSA must focus on improving its processes, oversight, and project management to address the remaining or any future recommendations or mandates in a timelier
manner. As we reported in October 2016, 33 of PHMSA’s 81 mandates (25 percent) remain unimplemented, as well as about half of NTSB’s 118 safety recommendations and 7 recommendations from the Government Accountability Office.

In addition, PHMSA is working to address our five recommendations to improve how the Agency implements mandates and recommendations and coordinates with other Operating Administrations involved with the transportation of hazardous materials—FAA, FMCSA, and the Federal Railroad Administration. For example, our work found that PHMSA has not adequately coordinated, as required by a DOT Order, 34 on rulemaking and international standards development with these agencies, limiting its ability to resolve disputes in a timely manner. PHMSA is working to address these issues through organizational changes. It is too soon to determine whether these plans, once finalized, will aid the Agency’s ability to meet mandates and recommendations in full and on time.

Conclusion

The safe and efficient movement of people and goods is vital to our Nation’s economic growth, global partnerships, and quality of life. We remain committed to assisting DOT and the Secretary as they work to improve DOT’s management of programs and resources and ensure the greatest return on investment to taxpayers. We will continue to play a leading role in helping the Department detect and prevent fraud. Our office has a strong record of identifying weaknesses and recommending enhancements to DOT’s internal controls to better oversee its programs and grants, particularly in large-scale infrastructure investments such as the American Recovery and Reinvestment Act of 2009 and Hurricane Sandy relief funds. We will continue to strive to find innovative ways to ensure the Department fully leverages the fraud detection and prevention resources at hand—such as mining and analyzing data to better predict high-risk areas for fraud, waste, and abuse.

I appreciate this Committee’s continued support to enable us to enhance our coverage of the Department’s safety programs, administrative and management assets, and information systems security. We look forward to providing you with any information you may require and pledge our support in promoting safety and efficiency and preventing fraud in any forthcoming infrastructure plans.

This concludes my prepared statement. I will be happy to answer any questions you or other Members of the Committee may have.

Exhibit. DOT OIG’s Ongoing Audits as of February 6, 2017

<table>
<thead>
<tr>
<th>Project Title</th>
<th>Objectives</th>
<th>Source/Requester</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOT’s Ongoing Audits as of February 6, 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Department-wide</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOT’s Implementation of MAP-21’s Acceleration of Project Delivery Provisions</td>
<td>Our objectives are to (1) provide a status of the Department’s actions to carry out MAP-21 Subtitle C provisions and (2) identify possible vulnerabilities in the Department’s implementation of these actions.</td>
<td>Required by the Moving Ahead for Progress in the 21st Century Act of 2012</td>
</tr>
<tr>
<td>DOT’s Use of Other Transaction Agreements</td>
<td>Our audit objective is to evaluate DOT’s use and management of Other Transaction Agreements.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td>DOT’s Implementation of the Improper Payments Elimination and Recovery Act of 2010 During Fiscal Year 2016</td>
<td>Our audit objective is to determine whether the Department complied with IPERA’s requirements as implemented by the Office of Management and Budget.</td>
<td>Required by the Improper Payments Elimination and Recovery Act of 2010</td>
</tr>
<tr>
<td>DOT OCIO Cybersecurity Funding</td>
<td>Our audit objectives are to determine whether DOT (1) adequately planned for its cybersecurity funding needs and (2) expended cybersecurity funds in accordance with congressional direction.</td>
<td>Self-Initiated</td>
</tr>
</tbody>
</table>

---

33 Insufficient Guidance, Oversight, and Coordination Hinder PHMSA’s Full Implementation of Mandates and Recommendations (OIG Report No. ST2017002), October 14, 2016.

<table>
<thead>
<tr>
<th>Project Title</th>
<th>Objectives</th>
<th>Source/Requester</th>
</tr>
</thead>
<tbody>
<tr>
<td>OST’s Benefit-Cost Analysis of the TIGER Grant Applications</td>
<td>Our audit objective is to assess the Office of the Secretary of Transportation’s (OST) policies and procedures for evaluating benefit-cost analyses in determining which TIGER grant applications are forwarded for further review.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td><strong>Federal Aviation Administration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAA’s Policies and Procedures for Hiring New Air Traffic Controllers</td>
<td>Our audit objectives are to identify (1) FAA’s justification for adopting the new hiring process and (2) the changes that have occurred in the hiring pool since the process was implemented.</td>
<td>Requested by the Chairmen of the House Transportation and Infrastructure Committee and the Subcommittee for Aviation, and Senator Nelson</td>
</tr>
<tr>
<td>FAA’s Runway Safety Initiatives</td>
<td>Our objective is to evaluate FAA’s progress in implementing initiatives to improve runway safety.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td>FAA’s Oversight of Suspected Unapproved Parts</td>
<td>Our objectives are to assess the effectiveness of FAA’s (1) process for monitoring and investigating suspected unapproved parts and (2) oversight of industry actions to remove unapproved parts from the aviation supply chain.</td>
<td>Requested by the Ranking Members of the House Transportation and Infrastructure Committee and the Subcommittee on Aviation</td>
</tr>
<tr>
<td>FAA’s Oversight of the Safety of Commercial Airline Flight Decks</td>
<td>Our audit objectives are to assess the effectiveness of FAA’s actions to (1) identify vulnerabilities to flight deck security and (2) mitigate identified flight deck vulnerabilities.</td>
<td>Requested by Senator Dianne Feinstein</td>
</tr>
<tr>
<td>FAA’s Progress With Implementing High-Priority NextGen Capabilities</td>
<td>Our audit objectives in this follow-up audit are to evaluate FAA’s (1) process for identifying risks to implementing the four prioritized NextGen capabilities and (2) actions to mitigate any identified risks.</td>
<td>Requested by the Chairmen and Ranking Members of the House Committee on Transportation and Infrastructure and its Subcommittee on Aviation</td>
</tr>
<tr>
<td>FAA’s Oversight of ADS-B Contract</td>
<td>Our audit objectives are to (1) determine whether the ADS-B contract provides FAA the ability to monitor whether the contractor is providing required ADS-B products and services and (2) evaluate FAA’s procedures for determining payments to the contractor.</td>
<td>Required by the FAA Modernization and Reform Act of 2012</td>
</tr>
<tr>
<td>FAA Terminal Modernization at Large TRACONs</td>
<td>Our audit objective is to assess FAA’s progress in ensuring STARS meets FAA requirements at the 11 large TRACONs and supports NextGen capabilities.</td>
<td>Directed by the House Committee on Appropriations</td>
</tr>
<tr>
<td>FAA’s Oversight of Regional Airlines</td>
<td>Our audit objectives are to evaluate FAA’s process for (1) identifying periods of transition and growth at regional carriers and (2) adjusting its oversight to respond to changes in regional air carrier operations.</td>
<td>Requested by the Ranking Members of the House Committee on Transportation and Infrastructure and its Subcommittee on Aviation</td>
</tr>
<tr>
<td>FAA’s Actions To Address ERAM Outages</td>
<td>Our objectives are to (1) assess the causes of the recent ERAM outages and assess FAA’s actions to address them and (2) determine whether tradeoffs were made to ERAM’s design requirements to meet revised implementation schedules, and assess the delivery of new NextGen capabilities called for in FAA plans.</td>
<td>Requested by the Chairmen and Ranking Members of the House Transportation and Infrastructure Committee, Aviation Subcommittee, and the Chairman of the Senate Committee on Commerce, Science, and Transportation</td>
</tr>
<tr>
<td>FAA’s En Route Automation Modernization Program Information Security Controls</td>
<td>Our audit objectives are to determine (1) whether FAA has effectively implemented security controls to address weaknesses identified during our prior review of ERAM and (2) what other security weaknesses, if any, have developed.</td>
<td>Requested by the Senate Committee on Commerce, Science, and Transportation</td>
</tr>
<tr>
<td>Project Title</td>
<td>Objectives</td>
<td>Source/Requester</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>FAA's Controller Scheduling Policies</strong></td>
<td>Our audit objectives are to (1) determine FAA's progress in adopting and implementing a scheduling tool and (2) identify any challenges that will need to be addressed to realize potential benefits.</td>
<td>House Appropriations Committee</td>
</tr>
<tr>
<td><strong>FAA's Process for Staffing and Placing Maintenance Technicians</strong></td>
<td>Our audit objectives are to evaluate FAA's (1) methodology for determining maintenance technician staffing levels and (2) process for placing maintenance technicians.</td>
<td>Required by the House 2017 Appropriations Report</td>
</tr>
<tr>
<td><strong>FAA's Management of NextGen Pre-Implementation Funding</strong></td>
<td>Our audit objectives are to assess FAA's procedures for (1) selecting, justifying, and measuring the outcomes of projects that received developmental funding and (2) overseeing the execution of these projects.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td><strong>FAA's Oversight of the Passenger Facility Charge Program</strong></td>
<td>Our audit objectives are to review FAA's oversight of (1) air carrier compliance with collection and remittance of PFC funds and (2) airport operator compliance with the use of PFC funds.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td><strong>FAA's Oversight of Air Carrier Check Pilots</strong></td>
<td>Our audit objective is to assess the effectiveness of FAA's processes for approving and overseeing air carrier check pilots.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td><strong>FAA's Award and Oversight of eFAST Procurements</strong></td>
<td>Our audit objectives are to evaluate FAA's processes for (1) awarding and (2) overseeing eFAST procurements.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td><strong>FAA's SE2020 Program Task Order Award and Oversight</strong></td>
<td>Our audit objective is to assess whether FAA's actions for awarding task orders and overseeing the SE2020 acquisition program were sufficient to meet its program mission.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td><strong>FAA's Oversight of Revenue Use at “Grandfathered” Airports</strong></td>
<td>Our audit objective is to assess FAA's oversight of grandfathered airports' compliance with Federal law related to airport revenue payments.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td><strong>FAA Controls Over Overflight Fees</strong></td>
<td>Our audit objectives are to assess FAA's policies and procedures for (1) accurately computing overflight fees, (2) granting exceptions appropriately, and (3) collecting or referring fees to Treasury for collection in accordance with Federal laws and regulations.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td><strong>Federal Highway Administration</strong></td>
<td><strong>FHWA's Use of the Emergency Relief Program To Improve Resilience</strong> Our audit objective is to assess FHWA's processes and guidance for incorporating resilience improvements into emergency relief projects to rebuild damaged highway infrastructure.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td><strong>FHWA Construction Force Account Oversight</strong></td>
<td>Our audit objectives are to (1) determine the scope and magnitude of force-account projects funded through the Federal-aid Highway Program and (2) assess FHWA's processes for overseeing compliance with Federal force-account requirements.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td><strong>Federal Motor Carrier Safety Administration</strong></td>
<td></td>
<td><strong>FMCSA's Commercial Motor Vehicle Driver Restart Study</strong> Our audit objective is to determine whether FMCSA's design and implementation of the restart study complies with the requirements of the act.</td>
</tr>
<tr>
<td><strong>FMCSA's Investigative Practices for High Risk Carriers</strong></td>
<td>Our audit objective is to assess FMCSA's processes for ensuring that reviews of motor carriers flagged for investigation are timely and adequate.</td>
<td>Required by the Consolidated and Further Continuing Appropriations of 2015. Also requested by Senator Dick Durbin</td>
</tr>
</tbody>
</table>
### Exhibit. DOT OIG’s Ongoing Audits as of February 6, 2017—Continued

<table>
<thead>
<tr>
<th>Project Title</th>
<th>Objectives</th>
<th>Source/Requestor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial Motor Vehicle Loading and Unloading Delays</td>
<td>Our objectives are to (1) assess available data on motor carrier loading and unloading delays and (2) provide information on measuring the potential effects of loading and unloading delays.</td>
<td>Mandated by the Fixing America’s Surface Transportation Act of 2015</td>
</tr>
<tr>
<td>Federal Railroad Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FRA’s Acquisition and Use of Monitoring and Technical Assistance Contractors for High Speed Intercity Passenger Rail Grant Oversight</td>
<td>Our audit objectives are to assess (1) FRA’s acquisition of MTACs through the Volpe National Transportation Center and (2) FRA’s management and use of oversight services provided by MTACs for HSIPR projects.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td>FRA’s Collection and Management of Railroad Safety Data</td>
<td>Our audit objective will be to assess FRA’s collection and management of railroad safety data.</td>
<td></td>
</tr>
<tr>
<td>Federal Transit Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTA’s Oversight of Major Capital Projects in the Western Regions</td>
<td>Our audit objectives will be to evaluate PTA’s (1) processes for identifying and assessing major capital projects’ financial risks, and reviewing and approving grantee financial plans and reports and (2) oversight of grantees’ mitigation of financial risks.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td>PTA Grantee: the Metropolitan Transit Authority of Harris County, Texas</td>
<td>Our audit objective is to evaluate METRO’s financial condition and capacity, including its ability to fund new services while maintaining current operations.</td>
<td>Mandated by House Appropriations Committee Report 114–129</td>
</tr>
<tr>
<td>PTA’s Oversight of Integrity Monitors for Recipients of Hurricane Sandy Disaster Relief Funds</td>
<td>Our audit objective is to assess PTA’s policies for the use of integrity monitors and evaluate the Agency’s oversight of integrity monitors.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td>Office of the Secretary of Transportation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office of Small and Disadvantaged Business Utilization Oversight of Small Business Transportation Resource Centers</td>
<td>Our audit objectives are to assess OSDBU’s (1) processes for establishing the Centers and (2) oversight of the Centers’ compliance with cooperative agreements and achievement of program objectives.</td>
<td>Self-Initiated</td>
</tr>
<tr>
<td>Pipeline and Hazardous Materials Safety Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHMSA’s Technical Assistance Grant Program</td>
<td>Our audit objective is to evaluate PHMSA’s award and oversight of TAG funds.</td>
<td>Required by the Protecting Our Infrastructure of Pipelines and Enhancing Safety Act of 2016</td>
</tr>
<tr>
<td>PHMSA’s Workforce Management</td>
<td>Our audit objectives are to determine (1) whether PHMSA has developed geographic allocation plans, identified expected retirement rates, and developed recruitment, retention, and training strategies for OPS to address gaps and challenges, such as hiring and time-to-hire challenges, and (2) whether previous periods of macroeconomic and pipeline industry conditions impacted the ability to fill OPS vacancies and the degree to which special hiring authorities, including direct hiring authority authorized by the Office of Personnel Management, could have alleviated such difficulty.</td>
<td>Required by the Protecting Our Infrastructure of Pipelines and Enhancing Safety Act of 2016</td>
</tr>
</tbody>
</table>
The CHAIRMAN. Thank you, Mr. Scovel, and thank you, all of you, for your remarks.

Inspector General Scovel, the FACT Act required the Secretary of Transportation to officially certify NHTSA’s implementation of all of the DOT OIG’s recommendations regarding improvements to the agency’s vehicle defect analysis process. Initially, then Secretary Foxx made the certification, but in response to my October 6 of last year, 2016, letter, your office reported that several of the recommendations remained open. In your testimony today, you noted that these recommendations remain open.

Are there areas where NHTSA can still improve its defect analysis?

Mr. SCOVEL. Thank you, Mr. Chairman. We appreciate the Committee’s interest, of course, in NHTSA and ODI, and I recall specifically this committee’s hearing back in June of 2015, hot on the heels of our audit report that found significant defects in the investigation and analysis section of NHTSA’s Office of Defects Investigations.

You’re right, of course, that the Department had money at stake in terms of closing all 17 recommendations from our June 2015 report. When Secretary Foxx made his certification, he correctly indicated that 12 had been closed, and five had been resolved. In audit terminology, that simply means that the Department and NHTSA had intended to close those remaining five.

In fact, in response to your question to my office, we’ve renewed our examination of NHTSA and, of course, determined that five recommendations remained unanswered. They were still open, so they were not closed, and this Committee was correct in essentially taking the Department to task for that.

Most of those open recommendations from that report had to do with the early warning reporting data. One recommendation had to do with the complaint review process in ODI. Those are all key, we assess, to ODI’s continued effectiveness.

Mr. Chairman, we also have two other open recommendations regarding ODI, and they stem from a report that we issued in the middle of 2016. We wanted to go back and look to an audit report that we issued to NHTSA in 2011, where we made a series of recommendations concerning their internal operations and pre-investigative processes. Two of those recommendations still remain open, and they have to do with the efficiency of NHTSA’s own testing and documentation procedures.

Taken as a whole, Mr. Chairman, all of those are going to be necessary for NHTSA to come to grips with the continuing challenges it faces regarding vehicle defects.

The CHAIRMAN. Thank you.

Inspector General Roth, in your testimony, you noted that TSA does not currently have, and I quote, “an intelligence-driven, risk-based” security strategy for all modes of transportation, specifically highlighting the challenges of securing surface transportation and maritime facilities. Over the past year, your office has recommended the development of a cross-cutting, risk-based strategy that ensures that TSA is considering risks to all modes of transportation and allocating resources appropriately.
What progress has TSA made in this area, and what are two immediate priorities you would like to see the new TSA Administrator address?

Mr. ROTH. Thank you for the question. We haven't seen a terrific amount of progress in this area, largely because the recommendations that we made were long-term and it will take some time for them to accomplish those recommendations, coupled with the fact that those reports are fairly recent in time.

I think the biggest thing that TSA can do is build a risk-based budget, which they have not done. Currently, about 80 percent of their budget goes to aviation transportation, and only about 2 percent or 3 percent goes to surface transportation. We think that doesn't reflect the risk, and what we would vastly prefer is them to do a sort of white sheet, blank sheet of paper risk assessment across all modes of transportation and then build a budget in accordance with that, but that is a long-term project.

The CHAIRMAN. Inspector General Lerner, you testified that the NSF needs to show continuing commitment to change the culture, in your words, in improving oversight of its fiscal management of large research facilities in order to maximize research investment. Your work in this area resulted in many new oversight requirements in the newly enacted American Innovation and Competitiveness Act.

What grade would you give NSF for implementing OIG, National Academy of Public Administration, and congressional recommendations?

Ms. LERNER. I think it's too early to give them a grade on implementation at this point. We are happy to see that they have guidance in place to address many of the issues that we have raised over the years through our recommendations and that the National Academy of Public Administration raised in its report. We are going to be looking right now to see how they are actually implementing that guidance since much of it is new, and we haven't had a chance to address the actions that they've taken and to see if things are actually working in accordance with the new guidance.

The CHAIRMAN. So the grade is incomplete?

Ms. LERNER. Correct.

The CHAIRMAN. All right. My time has expired.

Senator Nelson.

Senator NELSON. Mr. Chairman, I'm going to defer my questions so our members can go ahead and get their questions asked.

I just want to comment that so many of the things that you all have mentioned that you've been involved in, we have been totally involved in: perimeter defense on airports, Takata airbags, science, and so forth. And I just want an assurance from you all: will you agree or commit to immediately let the Chairman and me know if you face any future attempts to remove you from office for anything other than legitimate cause? Just go down——

Ms. LERNER. I will.

Ms. GUSTAFSON. Yes, Senator.

Mr. ROTH. Yes.

Mr. SCOVEL. Yes, Senator Nelson.

Senator NELSON. Thank you.
The CHAIRMAN. I think we have first up on this side Senator Blumenthal.

STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thanks, Mr. Chairman, and thank you for holding this hearing. Thank you all for your good work. You are ultimately the source of vigilance and enforcement against corruption and wrongdoing in our Federal Government without regard to partisan advantage and without respect to fear or favor from the President. You should be independent and assured of protection from the Congress and ultimately accountable to the American people. So I want to join my colleagues in thanking you for your vigilant independence but also asking you to report to us any attempts to impede or intimidate you in your vital work.

The outstanding recommendations, Mr. Scovel, with regard to NHTSA—those are significant recommendations, are they not?

Mr. SCOVEL. They most certainly are.

Senator BLUMENTHAL. And are there timelines for completing them?

Mr. SCOVEL. Yes. In fact, NHTSA has exceeded the timelines that we and they agreed to when we delivered our audit report to them back in 2015.

Senator BLUMENTHAL. Thank you.

Mr. SCOVEL. They're over time.

Senator BLUMENTHAL. Mr. Roth, you indicated that the security checks, the covert testing that you've done at airport checkpoints, have produced results that are, to quote you, “troubling and disappointing.” Those results are still secret, are they not?

Mr. ROTH. Yes, they are.

Senator BLUMENTHAL. Shouldn't they be disclosed?

Mr. ROTH. That is not a decision for me to make. Certainly, any time that you disclose these kinds of vulnerabilities, there is a risk that would be involved in there. But, again, the fact of classification is done by TSA and not by our office.

Senator BLUMENTHAL. Can those results be made known to members of this Committee in a classified setting?

Mr. ROTH. Absolutely.

Senator BLUMENTHAL. Well, I'm going to request that you make them known to us, that we schedule an availability.

Mr. Chairman, I certainly will avail myself of it. You're now engaged in another round of covert testing around the country?

Mr. ROTH. That’s correct.

Senator BLUMENTHAL. When will those results be done?

Mr. ROTH. We’re hopeful that we will get them out in the spring, or at least complete our testing in the spring, and then write up the report and then present that report to the Department, ultimately to the Congress.

Senator BLUMENTHAL. I understand that you do not use words like “horrendous” or “unacceptable.” That about as strong as you generally are is to use words like “troubling” and “disappointing,”
which sound to the ordinary person like an understatement. But that’s pretty strong language for you, isn’t it?

Mr. ROTH. It was. In our previous covert testing, for example, we stopped the covert testing about 80 percent of the way through because the results were so alarming that we thought we needed to brief the Secretary immediately. We did and got very positive results.

Senator BLUMENTHAL. So “alarming” is not too strong a word to use.

Mr. ROTH. Apparently not, yes.

Senator BLUMENTHAL. I am very concerned by the fact of the President’s announcement about your tenure and its potentially inhibiting effect on the work that you do and, especially, on whistleblowers. Whistleblowers perform an essential function for your offices as well as for law enforcement, do they not?

Mr. ROTH. They absolutely do.

Senator BLUMENTHAL. I want to ask all the members of the panel—and, unfortunately, time doesn’t permit me to give you a detailed opportunity to respond. But would you agree with me that the protections for whistleblowers ought to be strengthened? And we can just go down——

Ms. LERNER. Yes, Senator.

Ms. GUSTAFSON. Yes, Senator. I do not think the protections can be too strong. I think that whistleblowers have to be protected.

Mr. ROTH. I would agree with that.

Mr. SCOVEL. And I too would agree, sir.

Senator BLUMENTHAL. Let me ask you, Mr. Scovel—and this is a somewhat detailed question, but I think important. The President owns several planes, a 757; several helicopters; a small Cessna. They all require routine FAA inspections, and they’re all more than 20 years old. The Washington Post reported last month that agency officials at the FAA are afraid of reprisals from the new president if they fail to certify these aircraft as safe for flying. We all remember that one of the President’s planes, before he was President, lapsed last year—the registration lapsed last year, and it was temporarily grounded by the agency. Could you tell the Committee what you are doing to ensure that the FAA does proper inspections of the planes that are owned by the President and that the FAA’s safety office avoids any sort of abuse or compromise? Because the flying public deserves to know that the law is being rigorously enforced.

Mr. SCOVEL. Absolutely, sir. Our office has worked with FAA and provided oversight of FAA and its aviation safety inspection business for many years now. We have an active hotline operation center. As, of course, you know, we get over 5,000 contacts a year. To date, we have received no contacts from FAA and aviation safety inspectors pertaining specifically to President Trump’s aircraft or the inspection procedures that may apply to those.

However, I would like to go on record in this setting and speaking in response to your question, but aiming my remarks to anybody in the FAA who has to do with aviation safety, whether it’s safety inspections of the President’s aircraft or in any other capacity, that they know they can call on us. In 2008, we did some landmark audit work and investigation work as well specifically per-
taining to aviation safety inspections—allegations that FAA inspectors had been, in our terminology, overly collaborative with officials of Southwest Airlines, foregoing certain inspections, and as a result, aircraft were being flown with cracks in the fuselage.

We substantiated some of those allegations, but we also worked very closely with whistleblowers from within FAA's aviation safety division and provided testimony in hearings both in the House and the Senate along those lines. I can assure this Committee, and I wish to encourage anyone from FAA who has concerns about FAA's oversight of safety matters from A to Z, that our office is a place that they can turn.

Senator Blumenthal. Thank you very much.

Thank you all for your service to our Nation.

Thank you, Mr. Chairman.

The Chairman. Thank you, Senator Blumenthal.

Senator Wicker is up next.

STATEMENT OF HON. ROGER F. WICKER,
U.S. SENATOR FROM MISSISSIPPI

Senator Wicker. Thank you, Mr. Chairman.

Ms. Gustafson, you began your testimony talking about FirstNet. Let me follow up. As we know, FirstNet was established by the Fiscal Cliff Bill in 2012, tasking FirstNet with building and operating a nationwide public safety broadband network. RFPs were issued to the private sector entities last year. Am I correct that states do have the option to opt out of FirstNet network deployment provided these states build their own radio access networks?

Ms. Gustafson. That is exactly right, Senator. Once the RFP has been awarded and the details are out, the states are going to have the option to opt out and take the responsibility of building the network themselves with the requirement that they meet the FirstNet requirements. But, yes, there is an opt-out provision.

Senator Wicker. Particularly interoperability requirements.

Ms. Gustafson. Yes.

Senator Wicker. Now, on December 5, 2014, the Department of Commerce OIG issued a report discussing missteps the Board made following the establishment of FirstNet. OIG conducted an investigation following allegations concerning conflicts of interest and inappropriate contract procedures. In light of the December 2014 report’s findings, FirstNet entered into a Memorandum of Understanding pursuant to the Economy Act with DOC OIG.

On June 8 of last year, DOC OIG staff informed the Committee staff that FirstNet had decided to cancel the MOU, believing that the startup difficulties the organization had faced were now resolved. Am I correctly informed that, indeed, did take place, and as a result, will OIG continue to have a dedicated FirstNet team?

Ms. Gustafson. You are correct, Senator. My understanding is that it did take place, but that did not change our responsibilities or our intent on overseeing FirstNet. We still have a dedicated team. We are undergoing reviews now and again, as I had noted in my opening statement, when this contract is awarded for tens of billions of dollars, we will continue our oversight. The only wrinkle for us is that now it becomes something that we have to oversee
with the one-year funds that we are given by Congress. But it is——

Senator WICKER. And that’s the result, and the only result, of this cancellation of the MOU.

Ms. GUSTAFSON. It requires some shifting of priorities with our money. But FirstNet is a top management challenge, it is a huge risk, and it remains high on our list and subject to oversight by us, yes.

Senator WICKER. Does the OIG have cooperation not only from FirstNet but other parts of the Department of Commerce?

Ms. GUSTAFSON. Yes. My understanding is that we are having no issues whatsoever with cooperation either from FirstNet or from the other bureaus.

Senator WICKER. Keep us informed on that.

Ms. GUSTAFSON. Absolutely.

Senator WICKER. And, Mr. Scovel, let me ask you about unmanned aircraft systems. We’ve called it various things, but now I think the term we’re supposed to use is UAS. Is it true that although there has been demand for civil UAS operations, there is still no practical test that operators take?

Mr. SCOVEL. That is correct, Senator. Some operators are required to take a knowledge test, but not a practical test in terms of going out to the field and demonstrating that they can safely fly and operate a UAS or a drone.

Senator WICKER. Now, I’m told by my friends at Mississippi State University that there are a number of UAS Centers of Excellence which have test sites at 23 locations across the country, including Mississippi, North Dakota, Kansas, Indiana, and New Mexico, to name a few states represented on this Committee. Wouldn’t those be good centers to develop demonstration processes and provide the practical tests necessary?

Mr. SCOVEL. They very well might, and the Centers of Excellence that were created by Congress in FAA legislation several years ago were designed with just that in mind. FAA, I know, has encouraged industry and other stakeholders to consider using these Centers of Excellence for any and all purposes UAS related.

Senator WICKER. This is not a decision that requires statutory change, is it?

Mr. SCOVEL. I don’t believe it does. But what it does require would be continued partnership—and I say continued because FAA, to its credit, has engaged in substantial partnership already with the burgeoning UAS industry—but continue that partnership between FAA, industry stakeholders, and, of course, the Centers of Excellence themselves to see how the facilities and capabilities of the Centers might serve the needs of industry as they seek to grow the business.

Senator WICKER. Thank you, sir.

The CHAIRMAN. Thank you, Senator Wicker.

Senator Blunt is up next.

STATEMENT OF HON. ROY BLUNT, U.S. SENATOR FROM MISSOURI

Senator BLUNT. Thank you, Chairman.
Mr. Scovel, on the NextGen system, your office issued a report that chronicled some of the FAA’s failures in coordinating research and development for implementing that system. You said they lacked, “a clear process of identifying high priority R&D to support NextGen.” You made a number of recommendations as to what needed to be done to get this on track. Do you have any sense that any of these recommendations have been followed to date?

Mr. SCOVEL. Yes. Thanks for the question. NextGen has become a perennial concern of my office, the Secretary’s office, and, of course, FAA. It began its existence years ago after being billed as a transformational effort for U.S. airspace modernization. Since then, it’s become more of an infrastructure replacement program, if you will.

It has been a murky process almost from the get-go, and FAA, because of how it has contracted with the six transformational systems comprising NextGen, how it has segmented those into smaller and smaller pieces that don’t allow the Congress and the Secretary and industry stakeholders the opportunity to see how all of these will eventually link together, how much they will all cost, and what the benefits of the total package may be, and what the final scheduling may be—all of that has been uncertain. We’ve issued report after report with many recommendations. FAA has concurred and executed on most of those. Clearly, a lot of work remains to be done.

Senator BLUNT. Is it your view that this is just too big a project for them, or they can’t set the short-term goals that move us toward a conclusion? You know, this is constantly something out there that can’t seem to be accomplished.

Mr. SCOVEL. It has been a long, hard haul for FAA. I don’t, however, believe that it’s a matter, necessarily or inherently, beyond their capability. Due to some missteps perhaps early on in contract planning and acquisition management, FAA may have gotten off to a bad start.

Thanks to a partnership that I referred to earlier between an organization called the NextGen Advisory Committee and the agency itself, they now have a clear roadmap for the most immediate improvements to airspace management that can be provided through some of the NextGen initiatives. FAA is doing its best to execute on those. The timing certainly isn’t what industry would prefer, but there are certain aspects of the effort by FAA that are simply beyond FAA’s control or any other entity’s control if they were to assume responsibility for managing this part of NextGen.

Senator BLUNT. So does that mean the project is just too big?

Mr. SCOVEL. No, I don’t think it’s too big, sir.

Senator BLUNT. But you just said it was beyond anybody’s ability to control it. That sounds like to me it would be too big.

Mr. SCOVEL. Certain aspects of it. But what I meant to say—and thanks for allowing me to clarify it. For instance, when industry states its highest priority is the installation of performance-based navigation in its aircraft and at FAA facilities at airports—so that they can use curved approaches to land instead of having to come in with a straight-in approach, that’s great, and it will certainly help capacity and probably timing.
However, when communities in the vicinity of airports experience significant noise—new noise for the first time or at different hours—they do resist, they do protest, and they do bring lawsuits. It wouldn't matter whether FAA or another organization is presiding.

Senator BLUNT. All right. Let's talk about GPS for just a minute. In 2015, the Department of Transportation and the Deputy Secretary of Defense announced that they would be working to build an alternative system to GPS in case there is a disruption to the current system. Can you give me an update on that?

Mr. SCOVEL. I don't have an update on that, sir. I would need to get back to my office and communicate further with FAA. I do know that part of NextGen's allure is that it will move from ground-based radar up to——

Senator BLUNT. Well, now, I'm talking about—OK. Go ahead.

Mr. SCOVEL. Yes. The ADS–B system, which is a keystone of NextGen, is based on satellite technology and GPS. However, the Department now is exploring ways to use a multi-phased array radar, which may be the alternative—or at least a backup, providing some redundancy—to GPS satellites. FAA has a ways to go in order to be able to integrate this multi-phased array radar technology into air traffic control and the modernization effort. So I think that's what you're referring to.

Senator BLUNT. It is, and my question for the record will be if this commitment made in 2015—concerned about the current dependency that so many people have with GPS. Are they moving forward with a backup system if the current GPS system goes down? I don't remember the last time——

Mr. SCOVEL. Yes.

Senator BLUNT.—I looked at a roadmap. But I would hope I would have one if the GPS system no longer was there for me to rely on every time I go somewhere new and often when I go somewhere I've been before.

Mr. SCOVEL. Right.

Senator BLUNT. Thank you.

The CHAIRMAN. Thank you, Senator Blunt.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR, U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you for having this hearing.

I want to start out with one of the Executive Orders and how it has affected some of the airworthiness issues. There have been press reports that airworthiness directives that have been finalized by the FAA but not yet published in the Federal Register were pulled back after the White House issued the Executive Order freezing new regulations on January 20.

Mr. Šcovel, have you looked into this, and do you agree that airworthiness directives are really critical to safety and they should be released to the public?

Mr. SCOVEL. Airworthiness directives are absolutely critical to the safety of the flying public. And, in fact, we view them—and I
believe FAA does, too—as, in effect, a release valve or a safety valve.

When the President’s Executive Order suspended, at least—or whatever term may apply—the issuance of new regulations, new rulemakings, we were cheered because FAA, of course, had as an option in appropriate instances the capability to issue airworthiness directives. They customarily require a long lead time and extensive coordination with industry to make sure they get it right. But my understanding is that FAA may have paused on the issuance of ADs but intends to proceed with that and will use them in appropriate instances instead of rulemakings.

Senator KLOBUCHAR. Yes, I don’t think any new directives were issued until yesterday, which was two and a half weeks later.

Mr. Roth, in your testimony, you note that TSA is responsible for screening travelers and baggage for over 1.8 million passengers a day at 450 of our Nation’s airports. There’s an Executive Order freezing almost all Federal hiring. Reports indicate that there are significant concerns that this freeze applies to the TSA and could impact security and efficiency. In your view, how could the hiring freeze impact TSA and our homeland security?

Mr. ROTH. I don’t know whether it, in fact, applies to TSA or not. But, certainly, what we saw last spring was increased lines at checkpoints as a result of an insufficient number of transportation security officers. I think the line wait is highly sensitive to the number of personnel you have checking the baggage and checking the personnel, which I think is pretty much common sense.

Senator KLOBUCHAR. Ms. Gustafson, a similar question on the International Trade Administration. We worked really hard, a number of us, bipartisan, on steel dumping and trying to get those tariffs, which are very complicated, enforced. It has made a difference. We’ve brought back about half our iron ore workers, and I know Wilbur Ross in his hearing signified his commitment. How could a Federal hiring freeze impact the International Trade Administration’s ability to respond to increased steel dumping?

Ms. GUSTAFSON. Well, as you know, Senator, the International Trade Administration does have a compliance and enforcement arm that is charged with trying to enforce those laws. I have not looked into what the net effect would be as far as if there are going to be immediate impacts on the personnel. But, surely, less people working on enforcement would be a huge problem for the enforcement being done and being done in a timely manner.

Senator KLOBUCHAR. Thank you.

Mr. Roth, it has been widely reported that the Department of Homeland Security was not asked to provide technical assistance or guidance in the drafting of the Executive Order on refugees. In your role as Inspector General, you’re charged with ensuring integrity and efficiency at the Department of Homeland Security. Your office announced you will review the implementation of the Executive Order. In your experience, what’s the typical process for drafting and implementing policy that affects hundreds of thousands of people like this Order did?

Mr. ROTH. I don’t have any background on that. Our work in this area is simply going to be from the execution or the signing of the Executive Order moving forward. In other words, it’s going to be
specifically DHS-focused. What were they told, sort of, on the ground? When were they told it? When the court orders and the injunctions came in, how was that information communicated? And then as a separate piece, we’ll be doing misconduct investigations to the extent that we find officers or agents acting contrary to the instructions that they were given.

Senator KLOBUCHAR. OK. My last question here for all of you: As we enter a new administration with new leadership at your agencies, are you committed to exercising independent judgment in your investigations as you have done in the past?

Ms. LERNER. Yes, Senator, each and every day.

Ms. GUSTAFSON. Absolutely, Senator Klobuchar.

Mr. ROTH. Yes.

Mr. SCOVEL. Yes, we will, Senator.

Senator KLOBUCHAR. Thank you.

Senator CANTWELL. Thank you, Senator Klobuchar.

STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman. Thanks for having this hearing and thanks to all the witnesses this morning.

I always bring up this comment by the late Commerce Secretary Ron Brown that he was the Secretary of Commerce, but if he was getting a call from a Member of Congress, it was most likely about fish. In Mr. Ross’ confirmation process, he, in my office, said, “Yes, I’m having many conversations with my colleagues about fish.”

So I wanted to ask you, Ms. Gustafson—in your testimony, you clearly outlined the lack of stock assessments being completed by NOAA and the challenges that NOAA faces in ensuring how we move forward with various stakeholders if we don’t have those stock assessments. So my question is: What are some of the challenges that we’re going to face by not having—or not facing up to this issue of—stock assessments?

Ms. GUSTAFSON. Senator Cantwell, I am in the same boat—I hate to say boat since we are talking about fish—as Mr. Ross in that I, too, in the spring when I was going through confirmation was shocked to learn how crucial fish was as far as commerce, because it is not the first thing that comes to your mind if you are just beginning to know Commerce. I know that I did get some questions during my confirmation hearing about some concerns about the fisheries and the councils. Before I was confirmed, we actually had a request from Senator Blumenthal and other members of the Connecticut delegation about doing some work in that regard.

So I am still getting my arms around the fish assessment process. I do know that we have planned some work. It will be concerning the Gulf States Marine Fisheries Commission. But we will be conducting enhanced stock assessments of the fisheries in the Gulf, and that is going to allow my office to examine the stock assessment process. I am hoping that will help me have some answers for the members who this is so crucial to their economy and to their constituents.

Senator CANTWELL. I think your testimony has it right. You say, “NOAA continues to face challenges to ensure timely and accurate
assessments, providing consultation to stakeholders,” and so as you’ve learned and everybody has learned, these are big economic issues for various regions represented on this Committee. And without the proper stock assessments, we can’t make decisions about how to move forward on catch, which impacts jobs, impacts regional economies, and, obviously, impacts consumers, ultimately, as well.

I bring this up because I know that Mr. Ross also mentioned a lot of questions about making sure that international intervention in our fisheries market—that there were things that he wanted to do. So, anyway, one thing we can do is get stock assessments done. So we’ll be happy to follow up with you on that. But thank you for including it in your testimony.

Mr. Roth, one thing I wanted to bring up—we’ve talked about the TSA and airport lines, and Sea-Tac is one of the fastest growing airports, I think, 3 years in a row now. One of the things that we’ve used is the canine units. These are incredibly important, not just for ease of moving quicker TSA lines, but also as a deterrent. As we can see in the Belgium explosion and other instances, these dogs can detect those kinds of materials.

We are behind, though, or let’s just say the demand is outpacing our ability to train. Do you think we need to look at alternative training sites to meet the TSA standard?

Mr. Roth. I would agree with you that TSA has sort of been behind the curve with regard to canines. They are doing more and more of that. They’ve been shifting, for example, some canines from commercial, sort of, freight air to passenger operations. It works very well in conjunction with expedited screening where you don’t go through the AIT but you actually just go through the walk-through metal detector. But there are significant challenges, and there’s a significant ramp-up. So that is an area that I think TSA ought to be studying to see whether or not they need greater capacity.

Senator Cantwell. Or third-party testing sites?

Mr. Roth. Correct.

Senator Cantwell. OK. Thank you.

Mr. Scovel, NTSB just made a decision on the findings of the North Dakota accident, basically saying that the axle break was part of the issue. Do we need more enforcement of inspections in the transportation sector?

Mr. Scovel. We do. Are you referring specifically to rail and hazmat transport?

Senator Cantwell. Yes.

Mr. Scovel. Of course, yes.

Senator Cantwell. Crude by rail, specifically.

Mr. Scovel. Yes. FRA is challenged like all the safety regulators in the Department of Transportation to target most efficiently and effectively its limited inspector resources. It has to be a data-driven and risk-based analysis that determines where and how and how frequently those inspectors will be used. But, yes, more can be done, of course.

Senator Cantwell. Well, we’d like to follow up with you on more details to that. For those of us in the northern tier states with so much traffic and so much product and the issue of these explosions,
we definitely want to make sure we have ample people covering those inspections.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Cantwell.

Senator Inhofe.

STATEMENT OF HON. JIM INHOFE,
U.S. SENATOR FROM OKLAHOMA

Senator Inhofe. Thank you, Mr. Chairman. Let me share a thought with you for the benefit of our witnesses and those who may be here observing that we have a little bit of a problem in that we have nine members of this Committee who are also on Environment and Public Works. We're meeting at exactly the same time. Now, I chaired that Committee for a number of years, and this is a problem with this many, and I'm hoping we'll be able to change that. But that's the reason you see a lot of members coming in and going out.

One of the things we dealt with over there for a long period of time—and, quite frankly, it's differed between Democrats and Republicans on the Committee, but I'm a conservative Republican, and I chaired the Committee. So the over-regulation that we're dealing with on a regular basis—well, I see that in the jurisdiction of this committee, too.

So, Mr. Scovel, in any period of rapid technology changes, one of the problems I've seen is we're not willing to discard the old, and we continue on some of the older practices that we don't, you know, have anymore. A good example—in addressing our pipeline problems, our nation's regulatory framework—several decades ago, they established what they call a class location system rule for natural gas and pipeline operators.

Now, it has long since been superseded by new technology. They have something right now called the “Smart Pig” technology, where they can go in and measure the strength of the pipeline without having to go through the very expensive operation. Now, the problem is that even though they have the new technology that can be used, they're continuing to use the old technology.

So are there any other regulations in FMCSA that perhaps are no longer necessary but we have not had the foresight to do away with them? Any you can think of?

Mr. Scovel. Thank you, Senator Inhofe. I am aware of the example you just cited. It's perhaps the most glaring example of the problem that you just described. My office has not maintained, specifically with respect to FMCSA or, indeed, across the Department, any kind of inventory or list of regulations that may be outdated.

Senator Inhofe. Now, could you do that?

Mr. Scovel. We could, working with the Department, see what we could do by way of an audit report along those lines. I will say, too, that with regard to FMCSA, we have looked really at the opposite side of the coin that you described, and that has to do with FMCSA's ability to enact the rulemakings that, in many instances, were mandated by the Congress or by NTSB, and its inability to do so in a timely manner and in an effective way.

So it's really not the same problem that you described. We did extensive work on that over the last year-plus and found problems
with FMCSA's ability to do that. And, specifically, the material strength problem that you just described, which was the subject of a congressional mandate—FMCSA has not yet passed a final rule on that. But in conjunction with that, that would be an opportunity, specifically, on the older technology and the older——

Senator INHOFE. OK. Well, real quickly, I want to—I appreciate that very much. So let's have a chance to visit personally about this, because we have some other examples also.

Now, since 2008, the EPA and the DOT have taken an increasingly heavy hand in regulating the auto industry with greenhouse gas emissions standards and CAFE standards. And just days before President Trump’s inauguration, the EPA issued a final determination. It was about a year earlier than they were supposed to do it. It was supposed to be in 2017, but in October or November is when we anticipated that would happen. My personal feeling is that they did that, wanting to get it done before the change was made.

So I would ask you: How does EPA's sudden departure from the previously announced process for reviewing the requirements impact the ability of NHTSA to engage on this issue?

Mr. SCOVEL. I don't have inside knowledge on what EPA's actions or motivations might have been. However, with regard to DOT's part in CAFE rulemaking, clearly, now it appears the ball is in NHTSA's court, and they have the opportunity to move forward in appropriate ways. But they'll need to reconcile what they may be able to do now with what EPA has apparently done and see how they can advance.

Senator INHOFE. Well, all right. But what I'd request is that you look into that to see what problems came with the premature evaluation that they made.

The last thing—I know my time has expired. But for the record, I'd like to suggest that our drone technology is not as good as it is in some other countries. Just recently, Rwanda—their government enabled a drone company to begin delivering blood and plasma to rural clinics.

So there are a lot more things that we could do, and I’d just like, for the record, to have you respond as to what might be the problem in moving along with technology that we see in the U.K. and other countries and perhaps be able to do that here in this country.

Mr. SCOVEL. We'd be happy to take that question, sir.

Senator INHOFE. Thank you.

Senator INHOFE [presiding]. Senator Booker.

STATEMENT OF HON. CORY BOOKER, U.S. SENATOR FROM NEW JERSEY

Senator Booker. Thank you, Chairman Inhofe, and I agree with you wholeheartedly about the drone technology uses going on and the innovation outside of our country. We in America, frankly, should be leading on that, and I appreciate that.

I also want to thank the panel just for your work. You are truly extraordinary Americans that provide a vital role, especially to issues of safety and security, and I’m thankful for some of the commentary that’s already been made about our airports.

Mr. Roth, I would like to direct some questions to you from what I consider not only a frustrating experience, but something that I
think really goes at the core of our democracy and the checks and balances of our government. About a week ago, President Trump issued an Executive Order that temporarily banned the entry into the United States of people from seven majority Muslim countries—I’m sure you are aware. It temporarily halted the refugee resettlement program and permanently excluded refugees from coming into the United States from Syria.

This Order, called by many a “Muslim ban”—whether it’s an anti-refugee ban or whatever label you want to put on it—clearly triggered nationwide protests and legal challenges and is working its way through the courts right now. At the time the Order was released, I was here at a very curious tradition in Washington called the Alfalfa Club, and I left that when I heard about what was going on at Dulles Airport. I also had been informed that there had been in the state of Virginia a court order that was issued, a temporary restraining order, that specifically said that the people being detained—many of them were allegedly not just green card holders, but some of them, including children, were actually citizens of the United States who were being detained along with family members for hours at a time—have access to attorneys, but that court order was being violated.

When I got to Dulles Airport, the Executive Order clearly was issued. I had a copy of it in my hand and sought to meet with Customs and Border Patrol employees, but they declined to meet with me, and they declined to explain, frankly, why they were violating a Federal court order. My experience, though, was not unusual. In fact, press reports have indicated widespread confusion, and there’s evidence that officials in other places were ignoring court orders to provide counsel to immigrants or potentially to United States citizens detained at the airport in the wake of this Order.

So, Inspector Roth, you are a lawyer and former Federal prosecutor. Would you agree with me that if CBP officials were aware of a court order and failed to comply with the Order, then the court order factually was violated? Would you agree with me on that?

Mr. Roth. That’s my understanding as a lawyer. Obviously, it would have to be intentional, that is, knowing, in fact, that a court order existed and then choosing not to follow that court order, if that’s correct.

Senator Booker. OK. So when I arrived with Judge Brinkema’s Order in hand, which I showed to officials, it was shuttled back to Customs and Border Patrol. So I know that they saw the Order before refusing to meet with me. And I wonder, do you agree with me that if they saw that Order from a Federal judge, just factually—in your experience as a lawyer—that is a violation of that Order? If the facts that I’m relating to you are correct, and they saw the court order and still refused to allow lawyers back to meet with the people they were detaining, many of them for hours—that fact pattern is a violation. Correct?

Mr. Roth. Yes.

Senator Booker. Now, Inspector Roth, you opened a review into the implementation of this Executive Order regarding refugees and the seven countries that were involved, including a look at whether Federal officials engaged in misconduct or failed to comply with court orders. Can you just for a moment elaborate on your review
and specifically tell me that with the fact pattern I’ve relayed to you—what actions could you take to hold CBP officials accountable? What are the consequences for such violation?

Mr. ROTH. Sure. Our inquiry is two parts. One is a systemic inquiry. Who knew what when? How was the information transmitted to the field? At what times did the various ports of entry understand, one, the Executive Order, and then, two, the variety of different court orders as they came in. So that is sort of a systemic look that we’re taking.

But, as you note, we’re also taking a look at what we would call misconduct investigations, which is something that we do hundreds of times a year, is investigate instances in which an individual CBP officer engaged in misconduct, and, certainly, knowingly violating a court order would be, in my view, misconduct. So we are going to be looking at those things. It’s still very much in the early stages as to what it is that we’re looking at.

But the IGs don’t impose discipline on individuals. We would, of course, recommend to the Department or find facts and then give that to the Department for them to institute whatever disciplinary actions would have to be taken against individual members. Now, if there is a clear violation of law, we’ll refer that to the U.S. Attorney’s office and the Justice Department to determine sort of the appropriate stance there.

Senator BOOKER. Thank you very much, sir. My time has expired.

The CHAIRMAN [presiding]. Thank you, Senator Booker.

Senator Cortez Masto.

STATEMENT OF HON. CATHERINE CORTEZ MASTO, U.S. SENATOR FROM NEVADA

Senator Cortez Masto. Thank you. Thank you for joining us today. And let me first of all say thank you for what you do. It is such an important task that you undertake. I was the Attorney General for the state of Nevada, and one of the roles I had was the investigation and prosecution of waste and fraud in our Medicaid programs. So I know what you do is so important for the taxpayers, and it is important oversight.

One of the things, however, I want to talk to you about—and I’m going to throw one question out to all of you—which has been a concern of mine is cybersecurity threats that you have talked about and the concern that Federal agencies are not appropriately meeting these demands. Can each one of you talk about the agency that you’re overseeing and the concerns about whether and how they’re meeting those demands and what should be done or could be done to address cybersecurity threats?

Ms. LERNER. At NSF, as many of my other colleagues do, each year, we do an assessment of the agency’s information security program through the FISMA audits, and we have had many repeat findings over the years and, in particular, some relating to information security in Antarctica. The agency is aware of these issues, and we are engaged in constant communications with them about what can be done.

Some of the issues, especially those in Antarctica, will hopefully be addressed when they renovate the facilities down at McMurdo.
But it will be an ongoing area of back-and-forth between us and the agency to address these issues.

Ms. Gustafson. Thank you, Senator. At the Department of Commerce, exactly as at the Small Business Administration, where I was Inspector General before coming to Commerce, I see security as a top management challenge. I think that is across the board. We have done several reviews in this area, and what Commerce suffers from, again, tends to be similar to what other agencies have, which are legacy systems that are very hard to protect and just kind of longstanding problems when the ball continues to move, as far as, you know, the cybersecurity threats keep changing.

So the key for us is going to be for the Department to continue to make that a focus and for the message from the top to be that it is going to be taken seriously. I think that is going to be the best thing that Commerce can do, and it is certainly something we will continue to work on.

Mr. Roth. For DHS, we’ve been challenged because of the breadth of what it is that we do and the number of different separate organizations that don’t really work as a single team. I will have to say that the Department, for its own IT systems, has made considerable improvement in the last two years. But there still needs to be considerable work done.

For example, in our last report, with regard to the Department’s IT systems, we noted that they reduced the number of computer systems that were operating without an authority to operate, which is really like a driver’s license. It’s a certification by the head—the CIO that, in fact, this system meets all the requirements under Federal law for IT security. They reduced that by a significant percentage, but there are still 79 systems within DHS without authorities to operate, which is somewhat like flying a plane without an airworthiness certificate. It’s not something that you ought to do, because you have no assurances that that information is secure.

That’s one part of it. So they’re continually challenged there. They’re continually challenged with acquisition of IT, and we’ve done a lot of work with regard to that. If you can’t acquire the IT, you can’t secure it.

And then the third aspect we have within the Department is that they have the governmentwide responsibility for securing the dot-gov e-mail addresses, for example, and the dot-gov networks. They have a program called, “Einstein 3 Accelerated,” which is a significant program that’s supposed to be detecting intrusions and then rejecting them. We haven’t done work on that, but the GAO has done work on it that has been fairly critical of whether or not it, in fact, works.

So those are all our challenges as we move forward.

Mr. Scovel. Thank you, Senator. Cybersecurity for DOT is one of our top challenges and one that we are continually focused on. DOT is challenged, like every other agency in government. The technology moves very fast, like Inspector General Gustafson mentioned. Legacy systems always pose challenges, too. The number of recommended changes that we have made to the Department continually exceeds their ability to respond appropriately.

Across a number of cybersecurity domains, my techies, if you will, have cited problems for me and the Department. Risk man-
agement is one. Inspector General Roth mentioned systems operating without authorization. The same is true at DOT. The number has risen from 10 to 70 over all of our 450-plus systems in the Department since 2011. When it comes to identity and risk management, DOT, as well, is deficient. The PIV card or the multifactor identification capability that our ID cards provide—only 30 percent of the Department’s systems are enabled to require PIV card access to those systems.

Continuous monitoring of networks, which Inspector General Roth also mentioned for DHS, is a problem as well for the Department of Transportation. Incident handling and reporting—we have found significant instances both within the Department and, specifically, at FAA, which is a significant problem area for the Department and cybersecurity because of its independence and also because FAA’s air traffic control systems are critical infrastructure, as that term of art is used in the cybersecurity world.

When there was a significant fire at an air traffic control center—a high-altitude, long-distance center in Chicago—and the system had to shut down for a couple of weeks, that was an incident that was not reported to the Department of Homeland Security, for instance.

Finally, contingency planning. This would be one of my top three challenges for the Department. It keeps me awake at night. Fewer than—well, 14 percent of the Department’s systems have proper contingency plans, and they’ve been tested effectively. The other 86 percent are deficient, in our estimation.

Senator CORTEZ MASTO. Thank you. I see my time is up, but this is a concern of mine that keeps me up at night and that I don’t think we’re paying enough attention to.

So, Mr. Chairman, I know my time is up. I’ve got additional questions, if it’s all right to be able to submit those in writing.

The CHAIRMAN. Yes, absolutely.

Senator CORTEZ MASTO. Thank you.

The CHAIRMAN. Thank you, Senator Cortez Masto.

Senator Capito.

STATEMENT OF HON. SHELLEY MOORE CAPITO, U.S. SENATOR FROM WEST VIRGINIA

Senator CAPITO. Thank you, Mr. Chairman, and thank all of you.

I’d like to start with Inspector Gustafson of Commerce. I’m very proud of the role that my state of West Virginia plays as a backup facility for NOAA and, particularly, backing up some of the data and processing that the satellite receives, the GOES–R satellite.

You mentioned in your testimony the challenges that NOAA has faced in launching that, and it was postponed, and then I noticed that the next one that’s scheduled will not be launching for another year. I just wanted to sort of dig into that a little bit more. Can you summarize your thoughts and concerns about where this—obviously, it’s a concern to the everyday American, as this is satellite data that helps us predict flash floods, save lives and property, and other things? So if you could expound on that a little bit.

Ms. GUSTAFSON. That is exactly right. The NOAA satellites are crucial, not just so that you know if you need to wear a coat tomorrow. But it is a health, safety, and very big monetary issue. There
are two big satellite programs at NOAA, as you noted, the GOES and Polar System satellites, one system where the launch of the first JPSS was just pushed back again to September.

So some of the issues that happen when you begin to have these pushbacks is that there is a possibility of a gap in coverage, where some of the satellites up there are old and have exceeded their life already. They are still working, but they have exceeded their life expectancy. But that is coupled with the very, very large expense of these systems—billions of dollars. But I think what is crucial for NOAA is that it continues to take the lessons learned from each satellite so that it can be applied—because these are all a series of satellites and a series of very large acquisitions. One of the themes that you will see in our reports is that it is important that NOAA be understanding the risks, alleviating those risks, and making the adjustments needed such that the next satellite following is learning from some of the difficulties that these satellites have had that have caused them the slippage in their launch, for example.

Senator CAPITO. The impression I got from reading your testimony—I'm sorry I wasn't here when you all were giving your testimony—was that the last satellite that was delayed then had to borrow from the funding from the next satellite. Is that right? So it sort of stalls out not just the technical aspects of it, but the funding aspect of it as well?

Ms. GUSTAFSON. The funding is always tricky for the satellites because it is so much money; especially when we are in an environment where we are working under CRs. That has caused some difficulties for the satellite programs, where the funding is not available at the beginning of the fiscal year. That caused some difficulty with some of the satellite planning and the activities because they were working under a short-term continuing resolution. So NOAA is constantly, again, doing that balance of planning for the future but making sure that the work is getting done today.

Senator CAPITO. Right. I'd like to continue with you, please, on a different topic. In 2010, our state received $126.3 million in the BTOP program with funds through NTIA as a result of the American Recovery and Reinvestment Act, and we also received $42 million to construct an open access middle mile. Even with this investment, our state is ranked the lowest, if not the lowest, near the bottom, in terms of broadband deployment.

What kind of measurement of success—when you're flushing out $126 million—did Commerce do with these funds to find out they were being deployed for the actual purposes for which they were meant?

Ms. GUSTAFSON. Senator, I would like to give you a better answer than I could possibly give you right here with three weeks into my tenure.

Senator CAPITO. Yes, that's fair.

Ms. GUSTAFSON. I do know that the important thing on those issues, especially the BTOP grants, is they will have a direct impact and, again, hopefully will lead to lessons learned for the very big FirstNet program and the National Public Safety Broadband Network program. That is why we are doing some work, as I noted
in my written and my oral testimony, on that to make sure that, again, we are learning.

And I think, when I was looking at Mr. Ross' testimony when he was before you as the nominee, one of the things he said that kind of stuck with me was if it cannot be measured, it cannot be managed, which is something I actually had not heard before. But I thought that was actually a pretty insightful thing. I do not know whether he made it up, but I think it was a good thing.

So I think that whether there are metrics is something that is important to look at. I do not know regarding the BTOP program if my office before had looked at it.

Senator CAPITO. And just, finally, since I'm running out of time, Inspector Scovel—and I'm not going to ask the question. But, if I had the time, I would ask this question: What kind of deep dive has been done in terms of the intent of Congress to alleviate some of the permitting issues to make them concurrent rather than consecutive and to save money, time, and get more completed projects? I'll just submit a written question along that line to see where you are on that and where the Department is as well.

Mr. SCOVEL. Thank you. We do have some information that may help you.

Senator CAPITO. Thank you.

The CHAIRMAN. Thank you, Senator Capito.

Senator Cruz.

STATEMENT OF HON. TED CRUZ,
U.S. SENATOR FROM TEXAS

Senator Cruz. Thank you, Mr. Chairman.

Mr. Scovel, a few minutes ago, you raised the vulnerabilities at the FAA to cyber threats and cyber terrorism. Can you describe those vulnerabilities and what steps we need to take to guard against them?

Mr. SCOVEL. Some of the work that we've done, quite honestly, Senator, has been in the SSI arena. It's the sensitive security information. We'll be happy to provide that in more detail in a closed setting.

However, what I can say—and this is work that dates back a while that we've refreshed over the years—is that FAA essentially maintains two systems, two networks. One, on the administrative side, more open to the public, operates the agency itself. The air traffic control system is designed to be a closed environment and impenetrable to malefactors, if you will. In effect, my techies have been able to, through the administrative system, come right up to this supposed firewall between the two, between the administrative and the operating systems, and they concluded that had they wished to at the time, they could have entered the air traffic control modernization area.

So perhaps we could elaborate more on that with you in a closed setting. But that's the essence, that's the vulnerability, and FAA's air traffic control system has been designated critical infrastructure in the technical sense, and it's the only such system, I believe, within the Department of Transportation to merit that distinction. So it's absolutely critical.
Senator Cruz. Well, that certainly is dismaying. I would definitely like to follow up on the classified context. It’s not lost on anybody the catastrophic loss of life that a successful cyber attack on air traffic control could potentially lead to.

Let me shift to a related topic, which is in November of last year, your office issued a report on the FAA’s NextGen program. In that report, you found that despite the fact that the FAA has identified what it calls transformational programs intended to provide new capabilities for air traffic control, and despite the fact that it has invested over $3 billion in these transformational programs since 2007, the total cost, benefits, and timelines for the programs are still uncertain. My understanding is that the cost estimates for the programs are now somewhere in the range of $6 billion, with the time for implementation beyond 2020.

Can you please elaborate for the Committee on the problems you identified in your review of NextGen?

Mr. Scovel. Yes. I could speak for a long, long time about it, unfortunately, but I will keep it short. In fact, the numbers that you quoted, sir, can be updated. Even more recently, FAA’s total cost estimate—very tentative in our view at this point still—is $20 billion for the agency, with completion pegged between 2025 and 2030, perhaps.

Senator Cruz. And that’s a forward-looking estimate? Is that $20 billion new dollars?

Mr. Scovel. No, that would be total.

Senator Cruz. Total.

Mr. Scovel. Already invested from about 2003 on. For industry, about $15 billion more. Caveat that with the fact that several years ago now, an internal study to FAA, worst case scenario, pegged the total cost for NextGen at $100 billion to be split between the agency and industry. Right now, FAA cost and scheduled completion is still undetermined.

FAA, to its credit, has undertaken continued partnerships with the aviation industry and has determined to focus on four key priorities that could be completely in place perhaps by the early 2020s. And if that were to happen, that would be a significant benefit and advantage to the American aviation industry.

Beyond that, however, the ADS–B system, which is a cornerstone for the entire modernization effort, would still need to be finalized. That would push it into the middle 2020s, with requirements still to be determined, and without those key requirements, then the benefits to industry, who will have to equip—after all, it’s not just hardware that the agency is buying, but—

Senator Cruz. So two final questions. Can you describe the benefits to the country that NextGen modernization could provide? And you also made recommendations for better management within the FAA to produce NextGen. Can you describe those recommendations?

Mr. Scovel. Yes. The advantages are greater capacity, time and speed savings on the part of the flying public, arguably better enhanced safety across a number of vectors. If all of those were to come into place, the country would be much better served in terms of its air traffic control system.
Your second question, sir, had to do with our recommendations to FAA for improved management. We have issued them by the dozen. The agency has implemented many, many of them, with still others yet to go. We will continue to keep our eye on it and work with the agency to do all we can to advance the effort.

Senator Cruz. Thank you very much.
The Chairman. Thank you, Senator Cruz.
Senator Duckworth.

STATEMENT OF HON. TAMMY DUCKWORTH,
U.S. SENATOR FROM ILLINOIS

Senator Duckworth. Thank you, Mr. Chairman, for convening this very important meeting.
The Inspector General Act established IGs in our agencies to provide leadership and to promote economy, efficiency, and effectiveness in the administration of agency programs. The faithful execution of this duty requires political independence so that IGs and their staffs can properly prioritize and ferret out waste, fraud, and abuse wherever it may occur.

That’s why I was so gratified to see Inspector General Roth respond swiftly to my request for a comprehensive investigation into the Federal Government’s chaotic implementation of President Trump’s immigration Executive Order, more commonly known as the Muslim ban, an EO that the courts are now examining closely because it may not honor the protections the Constitution guarantees.

Mr. Roth, after this hearing, would you provide my staff with an update on how the investigation is going?

Mr. Roth. We can give you an update as to the general parameters, what it is that we’re looking at, and our proposed timelines, our estimated timelines. The specifics of the actual investigation—because it’s an investigation, we never want to sort of preview what it is until it’s finally over. But we’re happy to give you what information we can.

Senator Duckworth. Thank you. I appreciate that.

This question is for the entire panel. The administration is reportedly seeking to find cost savings by slashing program offices that politically or philosophically do not fit in their worldview or short-term political agenda. At Commerce, the administration is looking to eliminate the Minority Business Development Agency, the Economic Development Administration, the International Trade Administration, and the Manufacturing Extension Partnership.

At NASA, there are even reports that President Trump would entirely eliminate all climate research. At Transportation, they may be looking at phasing out the Federal Transit Administration, slashing Federal surface transportation spending, and eliminating operating subsidies to Amtrak and funding for TIGER.

Look, instead of draconian, politically driven cuts, I know that your work as IGs has led to the correction of wasteful practices and elimination of inefficiencies. Could each of you quantify or describe the savings and efficiencies that your oversight has resulted in within your own agencies, just some examples?
Mr. SCOVEL. Sure. Thank you, Senator. Our office—in the last fiscal year, our return on investment, if you will, was $54 to $1, which means that we were able to identify fines, restitutions, or recoveries on the criminal side, and on the administrative side, we were able to find recommendations for funds to be put to better use or question costs that, together, amounted to $54 for every appropriated dollar that came to the OIG, and that’s just, of course, within the Department of Transportation.

Within the Federal Highway Administration, one of our key findings and recommendations had to do with a $4.4 billion total package having to do with how that operating administration in DOT administers part of its grant program called Preliminary Engineering and how, essentially, money was being left on the table in the various states. So that’s a significant example, a key one.

Another one would have to do with delinquent debt. We did a study last year that determined that DOT’s delinquent debt, which comprises on the administrative side of things like civil penalties, payroll overpayments—on the other side, it had to do with other grants and loans that may have been offered by the department to states and localities. All together, that amounted to almost half a billion dollars in terms of delinquent debt that the department was not properly following up on and making efforts to collect.

So those are a couple of examples, and we would, again, marry that up with what our return on investment has been for the OIG, the taxpayer, and the department.

Senator DUCKWORTH. Fifty-four dollars for every dollar spent—that sounds like a good deal for the American taxpayer.

Mr. SCOVEL. Thanks.

Senator DUCKWORTH. Thank you for the hard work that you do. How is the hiring freeze affecting your ability to carry out your duties?

Mr. SCOVEL. Right now, we’re feeling a squeeze, but not too much, thankfully. However, as time goes on, it certainly will. Even beyond the hiring freeze, which, right now, as you know, has been labeled as temporary, we are most concerned about the longer-range budget problem. Seventy-five percent of my budget goes to payroll and salary and expenses for our people.

We have no hardware. We have no programs. We have no grants. What we are able to produce for you and for the Secretary in keeping with my statutory mission to keep you fully and currently informed is criminal investigations and audit reports. That’s produced by our people, and when we suffer budget cuts, that means fewer people. Inevitably, it means fewer audit reports and criminal investigations, which will impinge on your ability to stay fully and currently informed.

Sadly, our very recent experience in terms of sequestration with all of this—in my office, we imposed a hiring freeze that lasted about 18 months to get us through that without any furloughs or RIFs of our existing staff. We were successful in doing that. But it did mean that we had to put the squeeze on the audit reports that we were able to generate in response to requests and our own self-initiated work.

So it’s a prospect that I don’t look forward to. Of course, we’ll do what we have to, and I promise this Committee and others we will
do all we can with what we’ve got, but beyond that, it’s a physical impossibility. But thanks for your interest, though.

Senator DUCKWORTH. Thank you. I’m out of time. I would ask the other panelists to submit your answers for the record. But it sounds like you’re a good deal for the American taxpayer.

Thank you.

The CHAIRMAN. Thank you, Senator Duckworth.

I’m going to go to Senator Blumenthal again in just a minute. But I want to follow up, Mr. Roth, with a response to Senator Booker’s questions. You underscored that actual knowledge of a valid court order would be necessary to a finding of misconduct by a particular CBP officer. Would you agree that such inquiries are necessarily fact specific?

Mr. ROTH. Well, they’re absolutely fact specific, which is why we’re conducting the inquiry. We have agents flying out to the various airports that were affected by this to conduct interviews and understand, sir, what the timeline is, who knew what when, and how that works.

The CHAIRMAN. And I know you answered yes to Senator Booker’s question about his own efforts to transmit a court order to CBP. But would you agree that having a U.S. Senator hand a paper copy of a court order to a frontline employee or a non-lawyer would, at a minimum, be extraordinary and might necessitate some prudent checking with CBP’s chain of command before any action, or before any intentional misconduct should be imputed?

Mr. ROTH. We are going to investigate all the facts and circumstances behind this, and, typically, what we do is write a report that shows all the facts and circumstances, and then we transmit it to the Department for their assessment and determination of whether any discipline is necessary.

The CHAIRMAN. So you would check with their chain of command in the process?

Mr. ROTH. Right. As we do these interviews, obviously, we interview the individual CBP officer, but we’d also interview all the way up the chain of command so we have an understanding of the context by which all this happens.

The CHAIRMAN. All right. Thank you.

Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Mr. Chairman.

Mr. Roth, a court order is binding on all employees of the Department of Homeland Security, is it not?

Mr. ROTH. That’s my understanding, yes.

Senator BLUMENTHAL. Well, it’s a pretty simple question. It’s not a “gotcha” question. There’s no trick answer here. It is binding. It is binding not only on DHS employees, generally, but on the United States Customs and Border Protection officials, specifically. And would you agree with me that making an employee of the CBP aware of the law by anyone is a proper action?

Mr. ROTH. Again, this is highly fact specific. Like any kind of inquiry like this, as you know from your background, there are a lot of different circumstances. For example, there might be an advice of counsel defense, for example, that may play in. We simply don’t know, and I think it’s probably not particularly productive to speculate as to what the facts are going to show until we get the facts.
Senator Blumenthal. My office has received reports that numerous law enforcement officers at the Customs and Border Protection reportedly have been illegally arresting, detaining, and intimidating innocent individuals arriving in the United States. Are these activities ongoing, to your knowledge?

Mr. Roth. I can’t answer that question. I have no knowledge one way or the other as to whether that’s continuing as we go. I will say that these kinds of——

Senator Blumenthal. But you’ve received those reports?

Mr. Roth. We received a number of allegations, not simply a Senate referral, but we received a number of allegations from individuals as well as organized groups as to the conduct of CBP, which is why we opened the investigation. It’s really no different from the kinds of investigations we do every day.

Senator Blumenthal. Roughly, how many reports have you received?

Mr. Roth. I can’t estimate at this point.

Senator Blumenthal. Is it in the tens or the twenties or single digits?

Mr. Roth. It’s not single digits, but I really can’t give you an accurate answer.

Senator Blumenthal. So more than 10?

Mr. Roth. That’s my understanding as we sit here. It’s well more than 10, yes.

Senator Blumenthal. I’m not holding you to a number here. I’m just interested in the general volume of the complaints.

Mr. Roth. Right. And what we’re getting to is some nongovernmental organizations who are compiling various complaints by individuals who were affected by this and then transmitting those to us.

Senator Blumenthal. Wouldn’t it be helpful to have a clear pledge from the Department of Homeland Security and the Department of Justice as to the provisions of these court orders and a clear commitment to respect and abide by these rulings of the courts?

Mr. Roth. Our inquiry is going to be largely focused on those first 3 or 4 days. My understanding, again, just from reading the media, is that, in fact, that statement has been made, that there is a commitment to obey lawful court orders. But, again, it’s going to be highly fact-based, when people received knowledge of these orders and what they did as a result of those orders. That is going to be the focus.

Senator Blumenthal. And you’ll keep us informed about what the results are?

Mr. Roth. Absolutely.

Senator Blumenthal. Thank you.

Just finally, to follow the issue that Senator Nelson raised, I’ve been reviewing the letters that you sent to him in response to his inquiry to you, and I noted that each of you were informed that your services would be needed only on a “temporary basis,” and that was July—I’m sorry, January 13, 2017. Correct?

Ms. Gustafson. Senator Blumenthal, I was not contacted. Just to be clear, I did not receive a phone call or anything else.

Senator Blumenthal. You did not?
Ms. GUSTAFSON. No.

Ms. LERNER. And I also did not receive any information speaking about being retained temporarily. What I heard, ultimately, was that I was staying.

Senator BLUMENTHAL. Have you received anything in writing?

Ms. LERNER. No.

Senator BLUMENTHAL. Have you?

Ms. GUSTAFSON. No, Senator.

Senator BLUMENTHAL. Mr. Roth and Mr. Scovel, you were informed that you would no longer be needed, correct?

Mr. ROTH. Correct.

Senator BLUMENTHAL. And then you were subsequently informed that you would remain on the job?

Mr. ROTH. That's correct.

Mr. SCOVEL. In my case, Senator, I was informed, and I quote, that I was “being held over on a temporary basis.” That was late on the evening of Friday, January 13. The following Wednesday, the eighteenth, I was told verbally that I would be remaining in office.

Senator BLUMENTHAL. Who informed you? Was that Justin Clark who informed you on the thirteenth that you would be held over on a temporary basis?

Mr. SCOVEL. No, it wasn't. It was a member of the Presidential transition team for DOT. His name was Marcus Lemon.

Senator BLUMENTHAL. And in your case, Mr. Roth?

Mr. ROTH. It was the head of the DHS transition team whose name is Michael Dougherty.

Senator BLUMENTHAL. And who subsequently informed you that you would stay on the job?

Mr. ROTH. Mr. Dougherty, after I actually reached out to him that following Wednesday—was unaware of some of the developments that occurred, so he needed to get back with me. Took about an hour, and then he called me back and he basically said disregard the previous message.

Senator BLUMENTHAL. And in your case, Mr. Scovel?

Mr. SCOVEL. Again, it was Mr. Lemon. I was meeting with the transition team on an unrelated matter, and in a side bar discussion mentioned it again to Mr. Lemon, and that's when he gave me what I took to be reassurance that I would remain in office.

Senator BLUMENTHAL. Has anyone on this panel received anything in writing providing you with assurance that you will remain in your present position?

Mr. SCOVEL. I've received nothing in writing, sir.

Mr. ROTH. No, Senator.

Ms. GUSTAFSON. No, Senator.

Ms. LERNER. No, Senator.

Senator BLUMENTHAL. Wouldn't it be helpful to have something, given that you have been informed that your jobs may be in jeopardy, in writing?

Mr. SCOVEL. Perhaps. I should say I don't really need it. I recall back in 2009, I received nothing in writing, either, and I was in office as IG at DOT. Sir, my commission that hangs on the wall over my desk says that I serve during the pleasure of the President of the United States for the time being. I understand my individual
status simply to be on a day-to-day basis at the pleasure of the President.

I do understand that the Congress has important institutional and larger governmental reasons to be interested in the continuation of Inspectors General, and I greatly appreciate your questions along these lines. The scope of any removal action or the reasons for it are certainly of larger interest. For me, as an individual, though, it’s steady as she goes, business as usual.

Senator BLUMENTHAL. Well, I have far exceeded my time, and the Chairman, as usual, is very gracious and generous, and I appreciate it.

But I want to suggest that every Inspector General ought to be assured and given a commitment in writing that they will continue in office unless the President decides, for some reason relating to misconduct of that Inspector General, that he or she should be removed, because of not only the comfort level it will give you, but also the effect on morale and commitment of the people who work for you. And as much as we thank you for your service, I want to thank also the folks who work with you, because their service also is absolutely essential to keep government honest. This comment has nothing to do with Republican or Democratic administrations, but it’s the reason why I suggested that whistleblower protection should be enhanced and why protection for you should be made clear.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Blumenthal, and as I noted in my opening statement, I agree, and I think the IGs have confirmed that the transition team quickly corrected the comments about the IGs being held over temporarily. But as in any administration or multiple administrations, the Office of Inspector General ought to be something that is treated with respect indifferently, and I am grateful—we have, in the previous administration, the Obama administration, in its first months in power, fired an Inspector General at AmeriCorps during an investigation of a prominent supporter of the President, and that’s the kind of thing we don’t want to see happen. So I’m glad that you’re receiving confirmation that you’re going to stay in your positions and keep up the important and great work that you and your offices do.

I have one final question for Mr. Roth, and it has to do with something that happened just recently, and that is that TSA announced that this month, it will be limiting access to pre-check expedited screening lanes to travelers enrolled in a trusted traveler program. It’s basically removing those who may have had access through frequent flyer programs. We support robust vetting of pre-checked enrollees, but TSA has also struggled to expand the roles of those in the trusted traveler programs.

Will you commit to monitoring the impact of these changes on airport checkpoint wait times and long lines?

Mr. ROTH. This is the first we’ve heard of this. Obviously, this has been a matter of some concern for us—who is entitled to expedited screening and who is not. There used to be a fairly robust program of randomly selecting passengers to go through expedited screening. We thought that was an unacceptable risk. We asked them to take it out.
We had a number of recommendations with regard to expedited screening. As I sit here, I can't recall whether the frequent flyer mile people, who received it as a result of having a status in frequent flyers, was part of our recommendation. So I'll have to get back to you specifically.

But I may candidly have made a recommendation that those individuals who are unvetted in any other way—and they're different than, for example, trusted traveler programs that are run by CBP, for example, or Federal employees who have a certain level of clearance. Those who have a gold sort of frequent flyer status sometimes get expedited screening by the virtue of that and that alone. We are not 100 percent sure that that represents an acceptable risk. But I certainly will be happy to take your comments back.

The CHAIRMAN. Thank you. This is something that—we all saw examples of some of the long lines that occurred, and there has been an effort to try and move people more into the PreCheck Program. But we would also want to ensure that the programs that are used to expedite travelers through wait lines are ensuring that the people are vetted appropriately.

Well, thank you all for your testimony and for the great work that you and your offices do. You obviously get a very good return for the American taxpayer, and we appreciate that. We'll look forward to hearing from you again, I'm sure, in the future.

I would also say to any members—Senators who perhaps aren't here but I'm sure members of their staff are—that if there are additional questions that they want to submit for the record, get those in. And upon receipt, if we could have all of you respond as quickly as possible, that would be greatly appreciated.

So thank you so much for your time and for your testimony. And with that, this hearing is adjourned.

[Whereupon, at 12:05 p.m., the hearing was adjourned.]
APPENDIX

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO HON. ALLISON C. LERNER

Question 1. From 2011 until 2016, Lockheed Martin held the Antarctic Support contract, NSF’s largest. At that time Leidos took control of the contract. What is your assessment of Lockheed’s performance over its contract term? Are there improvements Leidos can make?

Answer. NSF, through the United States Antarctic Program, manages U.S. scientific research in Antarctica. The Antarctic Support Contract (ASC) was awarded to Lockheed Martin in December 2011 and is NSF’s largest contract, valued at nearly $2 billion over 13 years.

We have not conducted a comprehensive assessment of Lockheed’s performance over its contract term. Our 2015 audit that assessed the effectiveness of NSF’s oversight of Lockheed’s performance in ensuring the overall health and safety of USAP participants concluded that Lockheed’s performance was generally effective and did not recommend any significant improvements.

In 2016, Leidos Holdings, Inc. and Lockheed Martin’s Information Systems & Global Solutions business segment merged. Our FY 2017 audit plan includes an incurred cost of the Antarctic Support Contract and we are planning future audit work to examine issues related to the merger.

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 Director should take to increase the effectiveness of the agency’s cybersecurity programs?

Answer. The most important steps NSF could take to ensure that it increases the effectiveness of its cybersecurity programs, would be to devote sufficient resources to correcting security vulnerabilities and to follow up to be certain that the Foundation implements proposed corrective actions in a timely fashion to ensure the integrity of its information and systems.

NSF agreed with the six recommendations in our FY 2016 Federal Information Security Management Act (FISMA) evaluation to strengthen controls necessary to protect its data from unauthorized access. Significant recommendations included development of policies and procedures for privileged account access to ensure that the right people have the proper level of access to NSF systems and developing a process to ensure that system vulnerabilities are remediated in a timely manner. We received NSF’s corrective action plan in February 2017 and have issued a memo resolving the recommendations. The FY 2017 FISMA evaluation will assess NSF’s implementation of its proposed corrective actions.

The confidentiality, integrity, and availability of NSF’s data is crucial to NSF’s ability to fulfill its mission. Thus, it is essential that NSF manage information security risk effectively throughout the organization. Complicating this effort is NSF’s reliance on various technologies and service providers to support its Information Technology environment.

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 take several steps to ensure that our recommendations are discrete tasks feasible for NSF to implement in a reasonable timeframe. Our recommendations are tied directly to our findings, which we discuss with NSF management during the course of the audit. We also discuss recommendations with NSF management and may revise recommendations, as appropriate, based on the agency’s feedback to our draft report.

Once we issue a report, we communicate frequently with NSF management during the audit resolution process to help ensure that our recommendations are addressed in a reasonable timeframe. In 2010, OIG and NSF management established
a Stewardship Collaboration, comprised of staff from NSF’s financial division and OIG’s Office of Audits, which meets monthly to discuss current issues and identify possible barriers to resolving audit recommendations. This forum has helped resolve a number of audit recommendations more efficiently and helped ensure that NSF takes corrective actions in a timely manner.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DEB FISCHER TO ALLISON C. LERNER

Question. Inspector General Lerner, your testimony references the Intergovernmental Personnel Program. I am concerned that this program could be a significant source of waste, fraud, and abuse at the Foundation. For example, the Foundation has paid salaries of up to $440,000 for members of the program and has funded a significant amount of travel for them as well. What steps is the Foundation taking to reduce the risk of waste, fraud, and abuse in this program and where do you think they can improve?

Answer. In response to our 2013 and 2016 recommendations, NSF has taken steps to reduce IPA costs. In October 2016, NSF announced that it would start a pilot program to require institutions to contribute a 10 percent cost share for IPAs’ salaries and fringe benefits and NSF will eliminate lost-consulting reimbursements in new IPA agreements. In addition, in 2016 NSF limited IPA travel to the home institution under the Independent Research and Development Program to 12 trips per year.

As a next step toward lowering IPA program costs, NSF could evaluate other cost saving measures recommended in our 2013 and 2016 audits, including limiting the annualization of IPA salaries to comparable Federal pay rates and closely reviewing what it pays for IPA fringe benefits.

Our audits have not identified fraud in the salaries paid under the IPA program.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DEAN HELLER TO ALLISON C. LERNER

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 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. During my tenure as IG at NSF, my office has not had difficulty accessing information needed to hold NSF accountable. Additionally, the agency has not significantly delayed IG access to information or objected to IG access. I would add that the NSF Director recently reinforced OIG’s access authorities by re-issuing a directive to all staff, reminding them, among other things, to fully and promptly comply with all OIG requests for documents, interviews, briefings, and other information and materials.

We appreciate the Committee’s support for IGs in general and for our office’s oversight efforts to strengthen accountability and safeguard scarce Federal research dollars. We also grateful for the provisions in the Inspector General Empowerment Act that affirm and clarify IGs’ access to necessary information in a timely manner.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO ALLISON C. LERNER

Question 1. According to the Inspector General Act of 1978, the role of an IG is to detect and prevent waste, fraud, and abuse at Federal agencies and conduct these duties in a nonpartisan manner. IGs also have an obligation under the IG Act to keep Congress fully informed about issues at their agencies. Can I count on you to be nonpartisan and independent when carrying out your duties?

Answer. The National Science Foundation Office of Inspector General is an independent entity and reports directly to Congress and the National Science Board. As the NSF IG since 2009, I have always taken my responsibility to be nonpartisan and independent very seriously. As you know, Inspectors General are selected on the basis of their demonstrated expertise in areas outlined in the Inspector General Act of 1978, as amended, and without regard to political affiliations.
My office is committed to providing rigorous, independent nonpartisan oversight of the National Science Foundation (NSF). Our mission is to conduct independent audits and investigations of NSF's programs and operations and to recommend corrective actions to promote effectiveness and efficiency and prevent and detect waste, fraud, and abuse. Consistent with our statutory mandate, the OIG has an oversight role and does not determine policy or engage in management activities involving the Foundation or program operations.

**Question 2.** Can I count on you to keep me and this Committee fully informed about pending issues and whistleblower complaints at your agencies?

**Answer.** My office is committed to keeping Congress informed about pending issues and whistleblower complaints. With respect to pending issues, each year OIG identifies the most serious management and performance challenges facing NSF based on our audit and investigative work, general knowledge of the agency's operations and evaluative reports of others, including the GAO and NSF's various advisory committees, contractors, and staff. We articulate these challenges, as well as the progress NSF has made in responding to them, in our September Semiannual Reports to Congress.

In addition, our annual audit work plan summarizes the audits, evaluations, and inspections we hope to undertake during the upcoming year. Given the changing environment in which we operate, the audit work plan is meant to be a flexible document; we may modify it to address high-priority issues that come up during the year or to respond to requests from Congress, NSF, the National Science Board, or other stakeholders. We also meet regularly with congressional staff to discuss ongoing issues and emerging areas of concern.

Whistleblowers can be a valuable resource for exposing waste, fraud, and abuse. We take whistleblower complaints seriously and OIG educates NSF employees about whistleblower protections at presentations for new NSF employees; through information and resources on our public website; and by assisting NSF with annual Office of Special Counsel training. We will continue to keep the Committee informed about whistleblower complaints at NSF.

**Question 3.** A relatively stagnant budget means that the NSF has to make tough choices between maintaining older research facilities and bringing new facilities online. This year the NSF is considering divesting two older observatories—the Arecibo Observatory in Puerto Rico and the Greenbank Observatory in West Virginia. Both of these research facilities produce good science and can play a part in important missions, like detecting near Earth asteroids. Is there a robust process to make decisions about divesting facilities that considers all the benefits of maintaining these facilities?

**Answer.** Our Office of Audits plans to examine NSF’s decision process for divesting large research facilities as we continue our work focused on the Foundation’s cooperative agreements for large facility research projects. We started this work with audits of the proposed budgets to construct these projects. Pre-award oversight is especially important as the proposed budget for these projects, once approved by NSF, creates the basis upon which awardees can draw down advanced funds over the course of the award.

The audits disclosed serious deficiencies in the proposed budgets for these projects, which led us to examine NSF’s cost surveillance throughout the lifecycle of large facility projects. For example, audits of three of NSF’s large facility projects questioned $305 million in unallowable or unsupported costs out of $1.1 billion in total costs for the three projects.

We are currently broadening our work in this area to encompass cooperative agreements for the operations phase of large facility projects. As the next phase of this overall effort, we plan to examine the decommissioning process. NSF management and our office are currently discussing several decommissioning issues that arose from a prior audit, including determining which awardees have unfunded liabilities and the amount of those liabilities.

**Question 4.** The recent blockbuster “Hidden Figures” tells the true story of the women at NASA who played critical roles in the early days of the space program. Unfortunately, some of the challenges faced by these women in the 1950s remain today. Economists tell us we are facing a shortage of workers in STEM fields, yet women and minorities remain underrepresented in science and engineering. The Federal Government should be leading the way in promoting workforce diversity, and ensuring the best people are in each job, regardless of their gender or race. How would you characterize the NSF’s role in promoting diversity in STEM? Are there areas in which the NSF can improve?

**Answer.** It appears that NSF recognizes its important role in promoting diversity. For example, NSF’s February 2017 solicitation, the first under a new initiative to...
promote the inclusion of under-represented groups of individuals, stated that diversity is essential to achieving excellence in science and engineering research and education. According to NSF, a primary goal of this initiative is to transform STEM so that it is fully and widely inclusive.

At this point, we have not audited the effectiveness of NSF’s efforts to promote diversity in STEM. We are therefore not in a position to identify areas in which the Foundation could improve.

**Question 5.** For over 50 years, the NSF has managed U.S. scientific research and related logistics in Antarctica. Sometimes this includes providing medical care or emergency rescue services for personnel associated with non-governmental organizations, including tourists. This diverts government funding and assets away from support for research and may pose significant costs to NSF. Currently, U.S. tour operators and other non-governmental entities do not need to certify before traveling to Antarctica that they have put in place adequate insurance, contingency plans, and other arrangements to ensure health, safety, search and rescue, and medical care and evacuation for their expeditions. There are also no mechanisms to ensure that NSF is reimbursed in the event the Foundation renders emergency assistance. Do you believe the lack of an enforcement regime for contingency plans or reimbursement mechanism pose a risk to NSF’s Antarctic mission?

**Answer.** Diverting scarce Federal funds and resources to provide medical care or evacuations for private entities and individuals is a concern. While NSF has informed us that it has requested reimbursement for humanitarian/emergency support it has provided in the past, we have not done an audit or inspection to assess the cost or impact of such actions, or the extent to which NSF was ultimately reimbursed. Given the fact that Antarctica is a land governed by international treaty, there would likely be unusual challenges in seeking to create a formal enforcement regime for contingency plans or reimbursements.

---

**RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN THUNE TO HON. PEGGY E. GUSTAFSON**

**Question 1.** NOAA satellite acquisition has received considerable scrutiny in the past few years, including from this Committee. Several OIG and GAO reports have made recommendations on how to address the myriad schedule, cost, and functionality challenges for the $10.9 billion Geostationary Operational Environmental Satellite-R Series 4, and the $11.3 billion Joint Polar Satellite System 4 programs.

You noted in your testimony that NOAA’s major satellite system programs are among the Department’s largest investments, totaling more than 16 percent of its $9.7 billion Fiscal Year 2017 budget request. Do you believe NOAA will be able to avoid further cost overruns and delays in the acquisition process?

**Answer.** It is likely that there will be future cost overruns and delays in these programs. As we have generally reported in our work, the JPSS and GOES instruments are highly complex systems, and the small number of satellites procured by each program creates a challenge from a program standpoint. If any of the new satellites suffer a setback, those discrete delays have the potential to complicate ongoing and future work in the program resulting in cost overruns, particularly if technical problems arise during the satellites’ system assembly, integration, and testing.

The OIG’s past work concerning NOAA’s satellites highlights risks and areas of improvement to the Department, giving the programs an opportunity to learn and improve from past efforts—resulting in many resolved audit recommendations over time. The OIG will continue its work auditing these programs and keep Congress informed of the progress and challenges faced by NOAA.

**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 cybersecurity audits continue to find deficiencies in the Department’s implementation of basic security measures, such as regularly identifying vulnerabilities, expeditiously remediating security flaws, and effectively managing access controls. These basic measures are essential for improving the security posture of IT systems Department-wide, as is evidenced in our recent reports titled:

- Successful Cyber Attack Highlights Longstanding Deficiencies in NOAA’s IT Security Program;
- Lack of Basic Security Practices Hinder BIS’ Continuous Monitoring Program and Placed Critical Systems at Risk;
• Significant Security Deficiencies in NOAA's Information Systems Create Risks in its National Critical Mission; and

In the short term, the Department should prioritize some actions over others to improve the effectiveness of the cybersecurity program:
• fully utilize the Department’s enterprise security services at each bureau to gain real-time situational awareness;
• conduct high-quality information system security assessments to ensure adequate security is in place across the Department;
• prioritize the updating of IT security policies and procedures to ensure a cohesive approach to cybersecurity across the Department;
• implement strong security measures to protect the Department’s national security systems;
• implement multi-factor authentication for all users with greater authorities; and
• Secure cloud-based systems in accordance with Federal requirements.

**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.** With respect to recommendations contained in the OIG’s audit reports, consistent with GAO’s Government Auditing Standards, the OIG provides draft report findings and recommendations for review and comment by responsible Department management officials. The Department officials then have an opportunity to inform the OIG whether each recommendation is reasonable and feasible. If Department officials oppose any recommendations, and the OIG determines that the Department’s views are valid and supported, the OIG modifies the recommendations to incorporate the Department’s response in the final report. That final report, with the Department’s response, is then issued for implementation.

The OIG’s investigative reports generally are geared toward two audiences: the Department of Justice (DOJ) for potential criminal action or Department of Commerce (Department) management for potential administrative action. DOJ makes an independent determination as to the feasibility and viability of any criminal case arising out of OIG investigative efforts. Likewise, Department management makes the determination of what administrative actions, if any, are supportable by OIG investigative work. The OIG does not recommend specific action be taken in the administrative context as such decisions are within the Department’s management purview and not subject to OIG discretion. The OIG, does, however, highlight “root causes” of potential misconduct within the Department.

**RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DEB FISCHER TO HON. PEGGY E. GUSTAFSON**

**Question.** Inspector General Gustafson, in your written testimony, you highlighted more than $18 million in waste at the U.S. Patent and Trademark Office stemming from employees who falsified their timesheets. This is concerning, to say the least. Can you please discuss steps that have been taken by the Department to remedy this problem and any additional actions you think are necessary?

**Answer.** In its January 27, 2017, written response to the OIG investigative report finding more than $18 million in potential waste, USPTO reported taking actions to improve workforce management and strengthen time and attendance controls. Some of the recent actions USPTO reported that it has taken include:

• Providing guidance to patents and trademark supervisors to specifically monitor indicators of potential time and attendance issues, such as responsiveness to supervisory communications; inconsistent workload activity (e.g., claiming 80 hours of examining time in a bi-week, but not claiming any work credits); and customer inquiries or complaints;
• Implementation of an Agency-wide July 2016 policy requiring any employee with performance or time and attendance issues to provide more specific schedule information to their supervisor;
• Issuance of an USPTO-wide refresher on time and attendance obligations and training for all employees and supervisors on time and attendance policies;
• Launching a program to improve supervisory mentoring of patent examiners with low or inconsistent production;
• Providing guidance to all patent supervisors to regularly utilize their IT dashboard tool to monitor examiners’ production and timeliness, which can provide an early warning sign of potential time and attendance issues; and
• Additionally, the USPTO has implemented and/or taken action that responds to the 23 National Academy of Public Administration recommendations concerning internal controls related to time and attendance.

According to USPTO, some of its efforts to address the recommendations in the OIG’s report are ongoing, including:
• Reevaluating USPTO’s examiner production goals for each art unit and revising them, to the extent necessary, to reflect efficiencies in work processes from automation and other enhancements; and
• Reviewing USPTO’s policies, procedures, and practices pertaining to overtime hours to identify and eliminate the areas susceptible to abuse.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DEAN HELLER TO HON. PEGGY E. GUSTAFSON

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. Historically, the OIG has faced challenges gaining access to some information as a result of conflicting laws or occasional delays arising within the Department. The OIG has been successful enforcing our statutory right to have access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to the Department. More recently, the OIG encountered resistance from the Department in obtaining access to information protected by another statute. The OIG promptly informed Congress and the issue was resolved with full access being granted to the materials sought. As we move forward, we will continue to work with the Department to ensure timely access to all information needed to conduct our work.

At this time, the OIG has no current access issues. Should the OIG experience an access issue in the future, we will promptly inform Congress.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO HON. PEGGY E. GUSTAFSON

Question 1. According to the Inspector General Act of 1978, the role of an IG is to detect and prevent waste, fraud, and abuse at Federal agencies and conduct these duties in a nonpartisan manner. IGs also have an obligation under the IG Act to keep Congress fully informed about issues at their agencies. Can I count on you to be nonpartisan and independent when carrying out your duties?

Answer. Yes, nonpartisan independence is a cornerstone of effective oversight.

Question 2. Can I count on you to keep me and this Committee fully informed about pending issues and whistleblower complaints at your agencies?

Answer. I will keep Congress fully informed of fraud and other serious deficiencies relating to the programs and operations of the Department.

Question 3. The Commerce OIG website has a mechanism for employees to report “fraud, waste, abuse, or mismanagement,” at the Commerce Department. I assume that political interference or censorship of science within the department—like at the National Oceanic Atmospheric Administration (NOAA)—would qualify as something employees could report to your office. However, it might not be clear to employees that a violation of the scientific integrity principles—like censorship or muzzling of science—can and should be reported to your office. Will you put reporting information specific to scientists and other technical staff on your website so that “science is left to the scientists” as Mr. Ross, the nominee for Secretary of Commerce, put it?
Answer. The OIG maintains a robust website allowing all whistleblowers—regardless of subject—ready access to OIG staff. In addition, the OIG maintains a hotline for whistleblowers and other confidential tips with 24/7 access to live personnel for lodging confidential complaints regarding Department programs. Historically, the diversity of complaints received through these two mechanisms has shown that Commerce employees perceive both the hotline and the website as effective methods for confidential complaints to the OIG, regardless of the subject matter.

Question 4. Given the concerns about muzzling scientists or suppressing data, will you commit to immediately notifying this Committee of any whistleblower allegations of censorship, intimidation, or political interference?

Answer. As mentioned above, I will keep Congress fully informed of fraud and other serious deficiencies relating to the programs and operations of the Department. In that vein, I will report substantiated whistleblower allegations to the appropriate committees of jurisdiction.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CORY BOOKER TO HON. PEGGY E. GUSTAFSON

Question 1. When Congress authorized FirstNet, we required FirstNet to partner with the private sector. Congress purposefully gave FirstNet and its partners the flexibility to design and operate a first-of-its-kind network provided that the network met certain requirements such as infrastructure hardening and cybersecurity protections. As a practical matter, many of the challenges you identify with the program should be addressed after the private sector partner is selected. Do you agree with this analysis?

Answer. The selection of a private sector partner will begin to answer questions about the implementation of the first responder network. FirstNet’s actions addressing its challenges will be even more important after the private sector partner is selected. The OIG is committed to effective oversight of FirstNet during both the critical pre-award phase and the post-award roll out. Comprehensive oversight addressing identified challenges at their earliest point of detection ensures that FirstNet has ample time to deploy corrective actions likely to have the greatest impact.

Question 2. If so, do you agree that it be more appropriate to discuss these concerns after the award of the contract, once we fully understand its terms and FirstNet’s plans?

Answer. As noted above, the OIG believes that FirstNet must continue to address challenges as they arise. In partnering with the private sector, the processes established during the critical pre-award phase will have significant impact on the success of the post-award activities. Effective oversight of the FirstNet program must be broad and include all phases of operation to ensure a successful implementation of the statutory requirements.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO HON. PEGGY E. GUSTAFSON

Question 1. Does the Federal hiring freeze put in place by President Trump apply to your office?

Answer. Yes.

Question 2. If so, could this impact your ability to root out waste, fraud and abuse?

Answer. If continued for an extended period, it is foreseeable that the hiring freeze—coupled with spending held at FY 2016 levels—could have an increasing effect on the OIG’s ability to conduct timely audits or investigations. Additionally, certain statutorily required work must be completed each year regardless of funding levels. As funding remains constant and statutorily required work increases, fewer resources remain available for other work involving allegations of fraud, waste or mismanagement.

Question 3. Are there currently any open positions in your office that you are blocked from filling?

Answer. There are positions that do not specifically meet any of the exemptions specified in the hiring freeze guidance (Memorandum M–17–18) issues jointly by OPM and OMB on January 31, 2017.

Question 4. President Trump’s historic refusal to divest from his private companies and put his assets in a blind trust creates conflicts of interest across the Fed-
eral Government. This means that inspectors general could face new levels of work investigating improper use of public funds—or worse, investigating and reporting on corruption, waste, fraud, and abuse. Will you pledge to request from Congress adequate budget resources for Fiscal Year 2018 to fulfill your duties as Inspector General?

Answer. Yes.

Question 5. I am concerned about taxpayer dollars being used to promote President Trump's private businesses. There are news reports that taxpayers are on the hook for nearly $100,000 in Secret Service and embassy staff hotel charges for a two day Trump Organization promotional trip to Uruguay in January. Taxpayers may get stuck with the tab again for Trump family travel expenses related to the opening of a new Trump hotel in Vancouver, Canada and a new Trump International Golf Club in Dubai. It seems to me that any and all expenses related to President Trump's personal business should be paid for by those businesses, not by American taxpayers. The President and his family should have Secret Service protection. But the recent Uruguay trip highlights the significant conflicts of interest that exist due to the President's refusal to divest from his businesses and place the proceeds in a blind trust. Will you fully investigate and then report back to Congress on whether any Economic Development Administration, International Trade Administration, or other Department of Commerce resources are being improperly used to promote the President's private business interests?

Answer. The OIG is committed to reviewing allegations involving misuse of Department resources or abuse of authority by Commerce officials. The OIG will continue to work with the Economic Development Administration, International Trade Administration and the Department to ensure Commerce resources are utilized and accounted for appropriately. If the OIG determines that Commerce resources may have been misused, the OIG will take appropriate steps to review those allegations.

Question 6. Whistleblower complaints and hotline tips from Federal workers are important ways an Inspector General can uncover waste, fraud and abuse. There are reports that nearly 1,000 career State Department employees signed on to a “dissent memo” challenging President Trump's Executive Order banning immigration from seven Muslim-majority countries. Use of dissent memos in the State Department is protected activity. So, I am very concerned when—reacting to diplomats' use of a protected forum—White House press secretary Sean Spicer told them, “they should either get with the program or they can go.” It is hard to imagine these comments will not have a chilling effect on State Department employees who have a right to circulate a dissent memo and other Federal workers who are protected when reporting misconduct. Will you give me your assurance that you and your office will protect whistleblowers from any unlawful retaliation from the White House?

Answer. As indicated above, the OIG is committed to reviewing allegations involving misuse of Department resources or abuse of authority by Commerce officials made by whistleblowers. The OIG supports the various protections afforded whistleblowers and makes available a website for anonymously reporting allegations, a 24/7 complaint hotline, and a whistleblower ombudsman. These processes ensure and enhance whistleblower rights and protections of Commerce employees and contractors.

Question 7. What steps do you take to ensure Federal employees can confidentially report potential waste, fraud and abuse?

Answer. Complainants may submit confidential and anonymous complaints through the OIG Hotline, via our website or directly to OIG staff. The OIG does not routinely disclose the identity of complainants, unless either the complainant expressly consents or the IG determines that a waiver of confidentiality is unavoidable during the course of an investigation, as required by the IG Act.

Question 8. I was quite alarmed by news reports that the Trump transition team sought a list of all Department of Energy employees or contractors who have attended climate change-related meetings. This sparked fears of a potential purge of scientists based on their research. There are also news reports that Trump administration officials may be blocking the public release of information by EPA scientists. Will you assure the Committee that you will investigate if there are complaints of inappropriate political interference, intimidation or censorship of scientists at NOAA or other Commerce agencies?

Answer. As mentioned above, the OIG is committed to reviewing allegations involving misuse of Department resources or abuse of authority by Commerce officials.
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 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 e-mails. 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

2Under Secretary for Management Memorandum, Strengthening DHS Cyber Defenses (July 22, 2015).
3DHS 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
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 cyberattacks 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. 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 e-mail, 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 containing Representative Chaffetz’s personally identifiable information. DHS could better address insider threats by protecting against unauthorized removal of sensitive information via portable media devices and e-mail, 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. 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.

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.

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 

Secretary for Management Memorandum, Continuous Improvement of Department of Homeland Security Cyber Defenses (January 13, 2016).


USSS Faces Challenges Protecting Sensitive Case Management Systems and Data, OIG–17–01 (October 2016).

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).

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

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 e-mail notifies TSA personnel that documents responsive to an OIG request must first be “cleared” within TSA before being provided to the OIG. The e-mail 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 e-mail attached to the October 2016 e-mail, 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.
RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO HON. JOHN ROTH

Question 1. According to the Inspector General Act of 1978, the role of an IG is to detect and prevent waste, fraud, and abuse at Federal agencies and conduct these duties in a nonpartisan manner. IGs also have an obligation under the IG Act to keep Congress fully informed about issues at their agencies. Can I count on you to be nonpartisan and independent when carrying out your duties?
Answer. Yes.

Question 2. Can I count on you to keep me and this Committee fully informed about pending issues and whistleblower complaints at your agencies?
Answer. Yes.

Question 3. On February 1, you announced that you were starting an investigation into the Trump administration’s “implementation” of the travel ban for visa and green card holders from seven countries in response to a request from Senators Durbin and Duckworth and whistleblower and IG hotline complaints. As you know, the travel ban is subject of several court orders, including a Federal District Court order blocking its enforcement nationwide. As a result of this order and the subsequent fallout, it appears that several countries may be looking to pull back on negotiations to allow Customs and Border Protection pre-clearance facilities in their countries. Pre-clearance is helpful because it allows us to vet passengers before they get on a plane to the U.S. It also makes it easier for passengers when they get to their destinations, which is important in tourist destinations like Florida. As part of your investigation, are you looking into the potential impact on the pre-clearance program?
Answer. Our investigation will cover the implementation of Executive Order, “Protecting the Nation from Foreign Terrorist Entry into the United States.” In addition to reviewing its implementation, we will review DHS’ adherence to court orders and allegations of individual misconduct on the part of DHS personnel, including CBP agents. We will also consider adding other issues that arise during the course of the review. At present, our investigation does not include a review of the potential impact on the pre-clearance program, but we will consider adding the issue to our future audit work plans, depending on the status of the pre-clearance program and our audit resources.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CORY BOOKER TO HON. JOHN ROTH

Question 1. America’s surface transportation network, which includes numerous public transportation agencies, railroads, and bus companies, is an essential component of our Nation’s transportation system. Last year, in my home state of New Jersey, more than 1.6 million passengers passed through an Amtrak train station as part of their journey.1 There is a clear need to protect our surface transportation network from those who wish to do us harm. On September 18, 2016, a backpack with five homemade bombs exploded near the New Jersey Transit train station in Elizabeth, NJ during a police examination of the device. I am immensely grateful that no one was hurt. Unfortunately, this incident came one day after bombings in Seaside Park, NJ, and in Manhattan, where at least 29 people were injured.2 As you know, the 9/11 Commission made a series of recommendations for the Transportation Security Administration (TSA) to provide direction to the entities that secure our Nation’s surface transportation systems. In 2007, Congress passed legislation requiring TSA and other agencies to implement these recommendations. In December 2016, you testified to this committee that 8 years after this law was passed, TSA had failed to make any significant progress on a number of these requirements. Since your testimony two months ago, what progress has TSA made in issuing proposed regulations to secure surface transportation networks?
Answer. Since my testimony in December 2016, TSA has made progress in implementing the three outstanding passenger rail transportation regulations required by the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act). On December 16, 2016, TSA published two rulemakings in the Federal Register:
- Notice of Proposed Rulemaking for Security Training for Surface Transportation Employees (Security Training) and

---

In January 2017, TSA reported it anticipates issuing a Notice of Proposed Rulemaking for surface security vetting by the end of FY 2017. Based on TSA’s actions we were able to change the status of our audit report recommendations from unresolved and open to resolved and open.

Question 2. What are the potential consequences for the security of our Nation’s vast surface transportation networks if TSA does not take action to implement these recommendations as required by law?

Answer. As discussed in our audit report OIG–16–91, TSA Oversight of National Passenger Rail System Security, TSA’s ability to strengthen passenger rail security may be diminished without fully implementing and enforcing the requirements from the 9/11 Act. The absence of regulations also impacts TSA’s ability to require Amtrak to make security improvements that may prevent or deter acts of terrorism.

In the absence of issuing formal regulations, TSA uses a variety of outreach programs, voluntary initiatives, and recommended measures to assess and strengthen rail security for Amtrak and other rail carriers. However, these security initiatives are voluntary, and therefore, rail carriers are not required to participate or implement TSA’s recommended security measures.

Question 3. In your professional judgment, what will it take to get TSA to finally implement these recommendations so that our surface transportation entities can protect the people who use their services?

Answer. We believe that continued oversight—both by the OIG and Congress—is needed to ensure that these recommendations are successfully implemented.

Question 4. For several years, TSA has stated that the agency uses an intelligence driven, risk-based strategy for transportation security. In December 2016, you testified to the Senate Committee on Commerce, Science, and Transportation that a DHS Inspector General report found that TSA does not have a risk-based strategy across all transportation modes. In fact, TSA only has a risk-based strategy for our Nation’s airports, and only on the secured side of the airport. From your written testimony to the Committee today, I can only conclude that nothing has changed. You write,

We found that TSA does not have an intelligence driven, risk-based security strategy to inform security and budget needs across all types of transportation. In 2011, TSA began publicizing that it uses an “intelligence-driven, risk-based approach” across all transportation modes. However, we found this not to be true . . .

Additionally, TSA’s agency-wide risk management organizations provide little oversight of TSA’s surface transportation security programs . . . no entity at TSA places much emphasis on non-air transportation modes.

Can you explain the benefits of a risk-based strategy and how it differs from TSA’s current approach?

Answer. A crosscutting risk-based security strategy would help ensure that all transportation modes, not just air travel, consistently implement risk-based security. This would help TSA align limited resources effectively—placing necessarily finite resources against the greatest risk. To do otherwise compromises transportation security and may leave surface transportation vulnerable.

TSA’s current approach is essentially siloed; its security programs for the surface modes operate independently of the aviation mode. TSA’s Executive Risk Steering Committee, comprising the Office of the Chief Risk Officer and 10 assistant administrators, has overarching responsibility for defining strategy and managing risk TSA-wide. However, it focuses primarily on the aviation mode and provides little oversight of the surface transportation modes.

Question 5. What are the consequences for security—particularly surface transportation security—if TSA doesn’t use a risk-based strategy?

Answer. Without a crosscutting risk-based strategy for all transportation modes, TSA cannot ensure it consistently prioritizes security and resource allocation decisions to protect the traveling public and the Nation’s transportation systems. TSA spends massive amounts of money on air transportation and only a tiny amount on surface transportation. However, TSA does not know exactly where its greatest risks lie. Without a disciplined process to look at risk across all modes of travel, TSA may be spending its resources in the wrong place, leaving the traveling public less safe.
RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO HON. JOHN ROTH

Question 1. Does the Federal hiring freeze put in place by President Trump apply to your office?

Answer. Section 6(a)(5) of the Inspector General Act states that Inspectors General are to be treated as independent entities for purposes of staffing and training, and OMB Memorandum M–17–18, Federal Hiring Freeze Guidance, dated January 31, 2017, further clarified that “in the case of an Inspector General’s (IG) office, the Inspector General is considered the agency head for the purposes of determining which positions in the IG office are exempt” from the Federal hiring freeze. The IG, exercising his authority as an agency head under the Presidential Memorandum entitled “Hiring Freeze,” has determined that the OIG is exempt from the hiring freeze given the critical role the OIG plays in ensuring that the national security and public safety operations and programs administered by DHS are run effectively and efficiently, including investigating workforce integrity issues of the entire DHS population.

Question 2. If so, could this impact your ability to root out waste, fraud and abuse?

Answer. DHS OIG provides independent oversight over DHS programs and operations, including the significant public safety and national security missions of DHS’ largest components: CBP, ICE, the Coast Guard, TSA, FEMA, NPPD, and USCIS (particularly as it relates to their fraud prevention and national security functions). DHS OIG mitigates the risk of mission failure when it finds shortfalls and provides assurances of mission execution to senior leadership when no such shortfalls are found. Failure to fully staff our audit, inspections and investigative functions to provide that independent oversight would directly impact the ability of DHS to conduct national security and public safety responsibilities, and undermine public confidence in the fair administration of laws.

Question 3. Are there currently any open positions in your office that you are blocked from filling?

Answer. As stated in the answer to Question 1 above, we are exempt from the hiring freeze. However, operating under a Continuing Resolution has hampered our ability to grow to the level that the Department, OMB, and Congress have deemed appropriate to allow us to accomplish our critical mission. This level requires approximately 80 additional full-time employees. Moreover, the FY 2018 budget process has not followed the typical course, so we do not yet know whether we will have the resources we need moving forward.

Question 4. President Trump’s historic refusal to divest from his private companies and put his assets in a blind trust creates conflicts of interest across the Federal Government. This means that inspectors general could face new levels of work investigating improper use of public funds—or worse, investigating and reporting on corruption, waste, fraud, and abuse. Will you pledge to request from Congress adequate budget resources for Fiscal Year 2018 to fulfill your duties as Inspector General?

Answer. Yes.

Question 5. I am concerned about taxpayer dollars being used to promote President Trump’s private businesses. There are news reports that taxpayers are on the hook for nearly $100,000 in Secret Service and embassy staff hotel charges for a two day Trump Organization promotional trip to Uruguay in January. Taxpayers may get stuck with the tab again for Trump family travel expenses related to the opening of a new Trump hotel in Vancouver, Canada and a new Trump International Golf Club in Dubai. It seems to me that any and all expenses related to President Trump’s personal business should be paid for by those businesses, not by American taxpayers. The President and his family should have Secret Service protection. But the recent Uruguay trip highlights the significant conflicts of interest that exist due to the President’s refusal to divest from his businesses and place the proceeds in a blind trust. Mr. Roth, will you fully investigate and then report back to Congress on whether any Secret Service or DHS resources are being improperly used to promote the President’s private business interests?

Answer. Investigating whether President Trump’s use of DHS resources improperly promotes his personal business interests and presents a potential conflict of interest is beyond the jurisdiction afforded the DHS OIG by the Inspector General Act of 1978, as amended.

Question 6. Whistleblower complaints and hotline tips from Federal workers are important ways an Inspector General can uncover waste, fraud and abuse. There are reports that nearly 1,000 career State Department employees signed on to a
“dissent memo” challenging President Trump’s Executive Order banning immigration from seven Muslim-majority countries. Use of dissent memos in the State Department is protected activity. So, I am very concerned when—reacting to diplomats’ use of a protected forum—White House press secretary Sean Spicer told them, “they should either get with the program or they can go.” It is hard to imagine these comments will not have a chilling effect on State Department employees who have a right to circulate a dissent memo and other Federal workers who are protected when reporting misconduct. Will you give me your assurance that you and your office will protect whistleblowers from any unlawful retaliation from the White House?


In the last year, DHS OIG undertook a substantial reorganization and rebuilding of its whistleblower protection function by creating a new and dedicated WPU housed in our Office of Counsel. The WPU consists of the Whistleblower Ombudsman, a supervisory whistleblower investigator and two newly hired whistleblower administrative investigators. The WPU has primarily been responsible for intake and preliminary complaint review during this timeframe, while Special Agents from the DHS OIG Office of Investigations and attorneys from the Office of Counsel jointly conduct all whistleblower investigations that are opened.

**Question 7.** What steps do you take to ensure Federal employees can confidentially report potential waste, fraud, and abuse?

**Answer.** Whistleblowers can confidentially report potential waste, fraud, and abuse to the DHS OIG Hotline. The Hotline is a resource for employees to report allegations of employee corruption, civil rights and civil liberties abuses, program fraud and financial crimes, and miscellaneous criminal and non-criminal activity associated with waste, abuse, or fraud affecting the programs and operations of the Department. The DHS OIG website provides a link to the Hotline, as does the Department’s intranet, DHS Connect.

We recently sent out a Department-wide e-mail regarding reporting fraud, waste, and abuse. This notice encouraged employees to take a proactive role in improving DHS by reporting wrongdoing, and instructed them on how to report such information. The notice also notified employees of their rights under relevant whistleblower protection statutes, and discussed the OIG Whistleblower Protection Unit, which was recently established to review and investigate complaints of whistleblower retaliation.

DHS OIG educates all new agency employees about whistleblower protections shortly after they join the agency. The OIG Whistleblower Protection Ombudsman (WPO), who has primary responsibility for whistleblower protection training and education within the agency, provides training to all new DHS headquarters employees at the new employee orientations presented twice monthly by the DHS Chief Human Capital Office (CHCO). The WPO provides new employees an overview of his role and responsibilities, describes the elements of whistleblower protection and prohibited personnel practices, and educates the employees on their rights. At the training, new employees are provided with handouts prepared by the Office of Special Counsel (OSC) on each of these topics. DHS is in the process of scheduling training for new appointees, which will include OIG training on the Whistleblower Protection Act (WPA) and Whistleblower Protection Enhancement Act (WPEA).

Beyond the training received as part of new employee onboarding, each DHS employee must also complete No Fear Act training every two years, which provides training on employees’ rights and remedies under whistleblower protection and antidiscrimination laws. DHS employees in a supervisory role also receive additional whistleblower protection training. The WPO works closely with the DHS Under Secretary of Management’s Office, the DHS CHCO, the DHS Chief Leadership Officer Council, and the individual training officers at each DHS component agency to address whistleblower protections. He collaborates with these groups on the role of the Ombudsman in DHS, the development of training materials for all employees
through the DHS OIG website, and the delivery of mandatory whistleblower training materials to new and existing employees through the DHS learning management system.

The WPO works directly with OSC to ensure that the OIG is providing DHS employees and supervisors with the most current whistleblower protection training. In Fiscal Year 2016, the WPO, working with OSC, provided supervisory training on the WPA and WPEA that fulfilled the necessary requirements to achieve OSC 2302c certification for the DHS OIG. The OIG then worked to achieve certification for the entire Department. Training for this certification required all 28,000 DHS supervisors to complete online OSC training and pass an online quiz. The WPO then worked with CHCO to convert the quiz into the DHS learning management system, where it is now required training for supervisors every three years.

We have raised our profile within DHS as the entity to which whistleblower complaints are reported, and with effective results. It is our duty to protect these individuals from being retaliated against as a result of stepping forward and, as before, we remain committed to empowering and protecting agency whistleblowers.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN THUNE TO HON. CALVIN L. SCOVEL III

Question 1. As you know I recently sent a letter to FAA Administrator Huerta requesting a detailed status update on NextGen. The letter highlighted much of the work you and your office have done, and specifically cited points made in several of your NextGen reports. Do you have any comments on FAA’s response to my letter?

Answer. FAA’s response includes valuable perspectives on measures of success, lessons learned, and plans for the future. However, we note the fact that NextGen has been redefined—this is a theme from our work as well as the May 2015 National Academy of Sciences report. We would like to offer several observations about FAA’s responses.

• First, FAA states there is a misunderstanding or misconception based on our report about the planned enhancements to the En Route Automation Modernization (ERAM) program, which modernizes systems controllers rely on to manage high-altitude traffic and integration issues with other programs. Contrary to FAA’s comments, our report does not state that ERAM is broken but rather points to the integration challenges and the central role ERAM plays in critical NextGen efforts. Specifically, as we noted in our 2016 report on the transformational programs, FAA faces complex integration issues with ERAM and Data Comm for controllers and pilots to ensure that aircraft information can be displayed on controller displays and flight information can be transmitted from the aircraft to ground and FAA automation systems in the 2020 timeframe. We note that Data Comm is a joint FAA and industry NextGen investment priority.

• Second, FAA’s comment about our observations regarding insufficient industry outreach is inaccurate and outdated. We have long pointed to the importance of stakeholder involvement as an important factor for success. Our ongoing work recognizes the collaboration between FAA and the NextGen Advisory Committee (NAC) on the NextGen priorities. The four high priority areas, which include Performance-Based Navigation (PBN) and Airport Surface Operations, have the potential for significant benefits for users. The NextGen investment priorities represent an important but long overdue effort. We plan to issue a report on FAA’s risk-mitigation efforts for implementing the priorities this summer.

• Finally, we believe FAA’s comments about their response to our January 2016 report on FAA’s progress with using congressionally mandated reform recommendations are accurate, but need some updating. We made three recommendations to improve FAA’s management of major acquisitions and better meet the goals of its reforms, two of which are now closed. Our recommendation for FAA to identify and incorporate Federal and industry best practices and guidance for planning and acquiring major capital investments into their acquisition process remains open. We emphasize that FAA’s efforts to respond to our
recommendation will assist FAA in leveraging its reform authorities and achieve the efficiencies and productivity enhancements envisioned by the Congress to meet the Nation’s aviation needs and result in better outcomes with major acquisitions.

Question 2. In his response to my letter, Administrator Huerta wrote that, “when [NextGen] programs are measured properly against a positive cost-benefit analysis and [FAA’s] commitment to invest, [FAA is] now on or ahead of schedule with many of [its] large investment programs.” Do you share this perspective?

Answer. FAA’s statement requires some clarification about the costs and benefits of NextGen Programs. Each program is required by the FAA Acquisition Management System to have a cost-benefit analysis to drive investment decisions. However, as we reported in our November 2016 report, FAA NextGen Transformational Programs, there is considerable uncertainty about when each program will deliver benefits to airspace users, and many benefits remain unquantified. This is illustrated by two of FAA’s largest programs that have combined current cost estimates of $4.7 billion in Agency costs alone, which excludes airspace user costs to purchase and install new avionics and train flight crews.

- Automatic Dependent Surveillance-Broadcast (ADS–B): FAA has completed the ground-based infrastructure for the system and has mandated that airspace users must equip their aircraft with new avionics for ADS–B Out by January 2020. The benefits that FAA identified in its business case for the program depended on savings from the decommissioning of radars and the reduction of high-altitude separation standards (from 5 nautical miles down to 3 nautical miles). It remains uncertain when and if radars will be retired and if separation benefits from reducing separation standards will be realized. In addition, FAA has yet to quantify the benefits of ADS–B Out in congested airspace in the vicinity of airports in areas such as New York and Chicago.

- DataComm: FAA, in response to NextGen Advisory Committee recommendations, the Agency accelerated the implementation of digital messaging of pre-departure clearance capabilities to over 57 towers, 3 years ahead of its original schedule. However, the major benefit of the program will be in the high-altitude en route environment using digital messaging to reroute aircraft to avoid thunderstorms and other adverse weather. To complete this effort, FAA must modify its ERAM en route automation systems and train air traffic controllers, along with airlines equipping their aircraft and training their flight crews. FAA is planning to begin implementing this new capability in the 2020 timeframe. FAA has yet to quantify the productivity enhancements for the controller workforce, which could be significant.

Question 3. Many stakeholders in the aviation community cite funding stability as a past and ongoing concern with respect to modernization of the air traffic control system. Can we attribute the FAA’s difficulties over the last dozen years, as laid out in independent reports from your office as well as the Government Accountability Office, solely to funding uncertainty?

Answer. While funding uncertainty and the sequester in the 2013 time-frame has impacted FAA, as with all Federal agencies, a lack of funding has not materially affected the pace of NextGen or air traffic control modernization in general. Our work shows that other factors have contributed to problems with NextGen. These include unrealistic expectations, an inability to establish requirements for key capabilities (like ADS–B In and the display of information in the cockpit), and a lack of agreed-upon investment priorities. FAA and the industry now have a set of investment priorities, including DataComm and Performance-Based Navigation—a long overdue step. We note Congress has provided $7.4 billion from Fiscal Years 2003 to 2016 to FAA to invest in various NextGen programs. A significant majority of FAA NextGen funding ($6.7 billion) has been in its Facilities and Equipment or capital accounts.

Question 4. 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. By taking the following steps, the Department could greatly strengthen its cybersecurity programs:

1. Complete the implementation of PIV cards for logical access.

---

2. Identify, assess risk, and improve the oversight of shared controls among DOT networks.

3. Ensure all systems have adequate contingency plans and test these plans.

4. Take action to reduce the risk of the growing number of systems operating in DOT without executive authorization (currently 70 systems) and the high number of unresolved security weaknesses.

**Question 5.** 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.** Government auditing standards require that we make recommendations that flow logically from the findings and conclusions, are directed at resolving the causes of identified deficiencies and findings, and clearly state the actions recommended. Additionally, these standards specify that recommendations are effective when they are specific, practical, cost-effective, and measurable.

In addition to writing recommendations that adhere to these standards, we provide the audited agency with the opportunity to comment on the feasibility of our recommendations twice, first during the exit conference at the conclusion of the audit, and then again in their formal written comments to our draft report. Finally, to provide for recommendation closure in a timely manner, although audit standards do not specifically address the issue of timeframes, by DOT Order, the audited agency is required to provide a target date for completion for each recommendation once concurrence is reached. Depending on the complexity of the findings and recommendations, target dates may not be met, and new target dates may need to be established.

**RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ROY BLUNT TO HON. CALVIN L. SCOVEL III**

**Question 1.** In a 2015 letter to five members of the House Transportation and Infrastructure committee, the Deputy Secretary of Transportation and Deputy Secretary of Defense announced that an eLoran system would be built to protect the Nation from local and wide spread GPS disruptions. Why has the Department of Transportation taken no action on this?

**Answer.** We agree that it is important to have a backup system for GPS in the event of an intentional or unintentional problem with the system. However, we have not conducted any work on eLoran or the Department’s decision to not pursue a backup system. We have forwarded the question to the Department for any response that they may have on this matter.

**Question 2.** I understand that private entities have made proposals to the Department of Transportation and other departments to build a backup system for GPS using private funds. Why has the government not acted on these offers?

**Answer.** We have not examined the proposals made to the Department by the private sector for a backup to the GPS system. We have forwarded the question to the Department for any response that they may have on this matter.

**RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DEB FISCHER TO HON. CALVIN L. SCOVEL III**

**Question 1.** Inspector General Scovel, you mentioned in your written testimony that DOT’s "reported delinquent debt increased by over 300 percent from $170 million to $737 million" between 1999 and 2013. To me, these figures represent a massive mismanagement of critical transportation resources. What is the DOT doing to address delinquent debt recovery for financing programs such as RRIF and TIFIA?

**Answer.** In our delinquent debt report, issued July 2015, we addressed delinquent debt from RRIF and TIFIA ($984K and $6.2M respectively) and from other loan programs as well. Our specific recommendation for improving loan programs was that DOT develop or enhance policies and procedures for complying with their specific requirements for delinquent loan collections. These policies and procedures vary from program to program. However, overall weaknesses in this area remain present because DOT has not completed the required actions.

**Question 2.** Inspector General Scovel, you mentioned in your written testimony that the Pipelines and Hazardous Materials Safety Administration (PHMSA) has missed about 75 percent of its deadlines for Congressional mandates. This is unacceptable. Last year, Congress passed the Protecting Our Infrastructure of Pipelines...
and Enhancing Safety, or PIPES Act, which sought to study and reform how PHMSA oversees pipeline safety. Specifically, it re-prioritized outstanding Congressional directives from the 2011 PHMSA reauthorization, and gives PHMSA the ability to hire pipeline inspectors with greater flexibility. In your opinion, has PHMSA incorporated the recommendations from the PIPES Act into its oversight? What further recommendations do you have to reform PHMSA so the agency can complete its mandates on time?

Answer. The OIG has not specifically examined the extent to which PHMSA has incorporated recommendations from the PIPES Act into its oversight. However, in October 2016, we reported that an impediment to PHMSA’s timely action in implementing mandates and recommendations from NTSB/GAO/OIG was the lack of agency-wide processes, guidance, and oversight. More specifically, between 2005 and 2015, PHMSA’s two program offices, the Office of Pipeline Safety and the Office of Hazardous Materials Safety, were primarily responsible for mandate implementation. As we examined how these program offices implemented mandates, we found that staff rarely followed project management requirements, and there was little accountability for meeting deadlines—both internal and external.

To address the lack of processes, guidance, and oversight, we recommended that PHMSA develop a policy for mandate implementation. While we have not received information from PHMSA about its progress on this recommendation, PHMSA has made significant changes to its rulemaking process since we issued our report. Because many of PHMSA’s safety-related mandates require rulemaking activities, we are encouraged that these recent changes will better position the Agency to address regulatory mandates more efficiently.

We recently initiated an audit mandated by the PIPES Act related to PHMSA workforce management that should provide Congress better insight into the Agency’s oversight of pipeline safety. As part of our review of workforce management we are examining PHMSA’s efforts to hire inspectors. That work is currently underway, and we expect to report out later this year.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DEAN HELLER TO HON. CALVIN L. SCOVEL III

Question 1. 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. We have a good working relationship with the Department to access the information we require to ensure accountability. That being said, if we encounter delays and lack of timeliness in obtaining Agency documents, we work directly with Department officials at the proper level to resolve them. When appropriate, access and delay issues and their impact on the scope of our work are documented in our reports. We are not requesting any additional tools from Congress to increase transparency.

Question 2. Every year, our offices are flooded with requests from local government and transportation commissions on the assortment of discretionary grants that the Department is authorized to issue for specific transportation projects. Nevada has benefitted from some of these programs without a doubt—but there are some overarching concerns about how the Office of the Secretary reviews these applications from Administration to Administration. Regardless of who is in control of the executive branch, our local stakeholders should know what they need to do to compete for these Federal resources year after year.

It is my understanding that you have conducted an audit on the policies and procedures in place for TIGER grant applications—what types of safeguards can be put into place to ensure applications to all discretionary programs are reviewed on the merits and each application is given a fair shake?

Answer. Currently, our office is conducting an audit of the Office of the Secretary of Transportation’s (OST) policies and procedures for evaluating cost-benefit analyses in TIGER grant applications and plan to issue a report in early summer. Previously, on September 20, 2012, we issued a report—DOT Established Timely Controls for the TIGER Discretionary Grant Program, But Opportunities Exist to Strengthen Oversight (OIG Report No. MH201218)—that focused on OST’s manage-
ment and oversight of the TIGER program, including performance measures for determining economic and transportation-related impacts and (2) the policies and practices established for overseeing the TIGER projects once awarded. The report made seven recommendations to the Under Secretary of Transportation Policy to address vulnerabilities in the process for reviewing grants and documentation, capabilities to manage the TIGER program, and establish a methodology to identify program outcomes. OST completed implementation action on the last of these recommendations in January 2017. Of particular note is one recommendation directed at transparency, by establishing and implementing a systematic process for documenting significant management decisions involving the program and individual TIGER projects, including follow-up actions resulting from meetings with Department of Transportation agencies. We would view this as one key safeguard to put in place when reviewing grant applications.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TODD YOUNG TO HON. CALVIN L. SCOVEL III

Question 1. General Scovel, on August 20, 2015, your Office of Inspector General issued a report regarding the efficiency of FAA Air Traffic Control (ATC) towers. In this report, you found that the FAA regularly fails to analyze their internal databases to review cost data and potential productivity efficiencies. By the report’s estimation, this failure to review data cost the FAA as much as $142 million each year due to ATC tower inefficiencies. What recommendations do you have for this committee to ensure that the FAA regularly reviews their own data and extrapolates cost efficiencies through the ATC tower network?

Answer. The recommendation we made in that report remains open. Specifically, we recommended that FAA identify the factors contributing to greater resource use by the least efficient towers as compared with the relatively efficient towers identified in the report, and develop a plan for addressing those factors.

FAA only partially concurred with the recommendation in its formal response to the report. On July 22, 2016, FAA provided documentation of analyses undertaken in an attempt to fulfill the recommendation. We found FAA’s analyses inadequate, because they were too cursory to identify the factors driving differences in resource usage, let alone support development of a plan to address such differences.

We met with FAA personnel on October 5, 2016, and on February 16, 2017, to discuss what we would need from the Agency to close the recommendation. We also provided documentation on why their earlier response had been inadequate and additional information to help focus Agency efforts. Following the October meeting, FAA committed to a target action date of April 30, 2017. In the February meeting, they told us that they would probably ask for an extension after they had the opportunity to examine the additional information, but they have yet not done so.

While it would be fruitful in the future for FAA to analyze their data to identify inefficiencies, we are still waiting for the Agency to develop an adequate response to addressing the inefficiencies we have already identified.

Question 2. General Scovel, On April 5, 2012, your Office of Inspector General issued a report reviewing the utilization of ARRA funding and suggested methods for the Federal Highway Administration (FHWA) to increase competition for State DOT contracts and advance best practices for the awarding of those federal-aid contracts. To date the FHWA has completed the OIG recommended assessment, but failed to implement several specific policies regarding the confidentiality of bids, the implementation of performance metrics to assess state contract trends, and the sharing of best practices by State DOTs. What, if any, barriers currently exist that prevent states from sharing best practices and implementing policies that will result in increased competition for State DOTs?

Answer. FHWA has taken several actions to address our report’s five recommendations. One recommendation is closed, and four remain open. One of the open recommendations addresses the sharing of State best practices, and the FHWA has made some progress toward closing it. Before our report was issued, FHWA—along with the American Association of State Highway and Transportation Officials (AASHTO)—began a Survey on Construction Cost Increases and Competition. This survey was completed in May of 2012, and identified industry trends and best practices. In February 2015, FHWA completed its National Review of State Cost Estimation Practices, which also addressed our report recommendations concerning evaluating competition and establishing performance metrics. The AASHTO survey and National Review results were transmitted to the states by FHWA in order to share best practices. In addition, we have been informed by FHWA that it plans to update its “Guidelines on Preparing the Engineer’s Estimate, Bid Review & Evalu-
tion’ by September 1, 2017, as part of Agency efforts to address our recommenda-
tions and to implement performance metrics to assess State contract trends and
share best practices among State DOTs.

At the completion of the 2015 National Review, FHWA concluded that the cost
of keeping bidders’ names and estimates confidential outweighed the benefits, be-
cause it would require resource-intensive regulatory revisions to Federal law and
some State laws. Discussions concerning actions to close this recommendation are
ongoing; the next action date for closure is September 1, 2017.

Question 3. General Scovel, as you note in the Top Management Challenges for
FY17, the FAA continues to face significant hurdles as it attempts to implement the
Next Generation Air Transportation System (NextGen). The FAA fails to properly
define costs and meet delivery timelines for this program, impeding the implementa-
tion of this vital system. As Congress considers an FAA reauthorization bill this
year, what advice does your office recommend to ensure for the on-time and on-
budget delivery of NextGen’s performance based navigation (PBN) to the American
public?

Answer. While there has been some progress, FAA must continue to address key
areas to ensure an on-time and on-budget delivery of PBN flight procedures that
deliver benefits. This includes early outreach to communities to address potential
noise concerns and collaboration with airspace users and air traffic controllers
throughout the process. To maximize the benefits of PBN, our work shows FAA also
needs to deploy automated decision support tools to help controllers space and se-
quence air traffic close to busy airports. This is important because many airlines
are equipped with Required Navigation Performance technology that allows them to
fly advanced flight procedures, including curved paths into airport runways. How-
ever, FAA has been slow to deploy advanced procedures and controller automation
necessary to optimize benefits. Without these tools, it is difficult, if not impossible,
for controllers to manage the flow of air traffic in a (mixed equipage) environment
where some are using more advanced curved approaches and others are using
straight-in approaches. FAA is currently developing an automated tool for managing
airport arrivals, but will not begin deploying it until 2019 at the earliest.

Question 4. General Scovel, in a July 9, 2015 report, your office reported on the
Department of Transportation’s lax debt collection policies that left in excess of $700
million in uncollected delinquent debt. Through your office’s audit, you identified
that the DOT failed to comply with proper debt collection procedures on 66 percent
of all debt obligations collected. The report cites multiple failures in the DOT’s utili-
zation of the Enterprise Services Center (ESC) that inhibit their ability to accu-
rately report on delinquent debt. Could you please outline what immediate actions
should be taken to ensure the Department reports debt by statutory timelines, im-
proves training for the proper collection of the Department’s debt, and ensures for
the full compliance to standard operating procedures for the department’s ESC per-
sonnel?

Answer. In our delinquent debt report issued July 2015, we made six actionable
recommendations, which remain open, to address DOTs weaknesses in identifi-
cing, reporting, and recovering delinquent debts. These included developing and imple-
menting department-wide policies and procedures for accurately identifying and re-
porting delinquent debt and recoveries, and collecting debts in a timely manner; es-
ablishing clear policies and guidance for overseeing delinquent debt collections
made by Operating Administrations and ESC; requiring relevant training for all
personnel who are responsible for identifying, collecting, and reporting on delin-
quent debt; directing Operating Administrations that must comply with legal re-
quirements outside of the Debt Collection Improvement Act to develop clear and ef-
fective debt collection policies and procedures for their unique requirements and to
share these policies and procedures with ESC; directing ESC to clarify its standard
operating procedures (SOPs), including (a) delineating the different processes for ad-
ministrative and loan debts and (b) identifying the Operating Administrations that
the SOPs apply to and; directing Operating Administrations that have loan pro-
grams to develop or enhance policies and procedures for complying with their spe-
cific requirements for delinquent loan collections.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO
HON. CALVIN L. SCOVEL III

Question 1. According to the Inspector General Act of 1978, the role of an IG is
to detect and prevent waste, fraud, and abuse at Federal agencies and conduct these
duties in a nonpartisan manner. IGs also have an obligation under the IG Act to
keep Congress fully informed about issues at their agencies. Can I count on you to be nonpartisan and independent when carrying out your duties?

Answer. Yes. Since taking on my role as DOT Inspector General in October 2006, I have been steadfastly committed to working with Congress, particularly with the Senate Commerce Committee, and with the DOT Secretary to help ensure that my office fully executes its mission to provide independent and objective reviews of DOT programs and operations.

Question 2. Can I count on you to keep me and this Committee fully informed about pending issues and whistleblower complaints at your agency?

Answer. As mandated by the Inspector General Act, I will keep the Congress and the Secretary fully and currently informed about problems and deficiencies relating to the administration of DOT's programs and operations and the necessity for and progress of corrective action. We will comply with the direction and privacy protections afforded to whistleblowers by whistleblower protection statutes and will, as appropriate, inform the Committee about whistleblower complaints.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO HON. CALVIN L. SCOVEL III

Question 1. Does the Federal hiring freeze put in place by President Trump apply to your office?

Answer. Yes.

Question 2. If so, could this impact your ability to root out waste, fraud and abuse?

Answer. I understand the President's desire to review current staffing levels across Executive Branch agencies. In fact, we are currently undertaking our own workforce assessment in an effort to apply our resources most effectively. Such assessments are a sensible best practice.

One thing that will remain at DOT OIG is our reliance on the specialized expertise of our workforce, which consistently amounts to at least 75 percent of our budget. Or put another way; our budget equals people, and people equal product. Sustained funding that allows us to develop and maintain well-qualified auditors, investigators, and subject matter experts is critical to our success. If the Administration and Congress commit to a significant infrastructure investment, such sustained support allows us to have meaningful oversight in place right from the start. Depending on the scope, timing, and direction of any such program, additional dedicated oversight resources, as were found in the Recovery Act and the Hurricane Sandy Disaster Relief Appropriations Act, may also be needed. Otherwise, the likely result would be DOT OIG pulling staff from other high priority areas in order to meet the challenges inherent with that new investment. Such a redirection of existing OIG resources could delay our efforts to meet other congressional mandates.

The oversight that DOT OIG provides demonstrably helps prevent fraud, waste, and abuse of taxpayer dollars. In Fiscal Year 2016, that amounted to a return on investment of $54 for every appropriated dollar; over the last 5 fiscal years, the average was $35 to $1.

Question 3. Are there currently any open positions in your office that you are blocked from filling?

Answer. No.

Question 4. President Trump’s historic refusal to divest from his private companies and put his assets in a blind trust creates conflicts of interest across the Federal Government. This means that inspectors general could face new levels of work investigating improper use of public funds—or worse, investigating and reporting on corruption, waste, fraud, and abuse. Will you pledge to request from Congress adequate budget resources for Fiscal Year 2018 to fulfill your duties as Inspector General?

Answer. Yes.

Question 5. Whistleblower complaints and hotline tips from Federal workers are important ways an Inspector General can uncover waste, fraud and abuse. There are reports that nearly 1,000 career State Department employees signed on to a “dissent memo” challenging President Trump’s Executive Order banning immigration from seven Muslim-majority countries. Use of dissent memos in the State Department is protected activity. So, I am very concerned when—in reacting to diplomats’ use of a protected forum—White House press secretary Sean Spicer told them, “they should either get with the program or they can go.” It is hard to imagine these comments will not have a chilling effect on State Department employees who have a right to circulate a dissent memo and other Federal workers who are protected...
when reporting misconduct. Will you give me your assurance that you and your office will protect whistleblowers from any unlawful retaliation from the White House?

Answer. As we have historically done with all whistleblowers, yes, we will continue to do our part to protect them from unlawful retaliation and comply with the requirements in the whistleblower protection statutes.

Question 6. What steps do you take to ensure Federal employees can confidentially report potential waste, fraud and abuse?

Answer. We offer several ways for Federal employees to report potential waste, fraud, and abuse confidentially, including anonymously if they so desire. DOT OIG operates a Hotline (www.oig.dot.gov/hotline) that is staffed 24 hours a day, 7 days a week, 365 days a year. We also have a Whistleblower Protection Ombudsman who helps educate U.S. DOT employees about prohibitions against retaliating against Federal whistleblowers. Our Office of Investigations provides fraud prevention briefings to various individuals including regional DOT employees and contractors, which include information about the various ways to alert OIG to allegations of fraud, waste, and abuse.

Question 7. I was quite alarmed by news reports that the Trump transition team sought a list of all Department of Energy employees or contractors who have attended climate change-related meetings. This sparked fears of a potential purge of scientists based on their research. There are also news reports that Trump administration officials may be blocking the public release of information by EPA scientists. Will you assure the Committee that you will investigate if there are complaints of inappropriate political interference, intimidation or censorship of scientists at NHTSA or other DOT agencies?

Answer. Yes. As with any complaint that we may receive, including those about DOT employees who may be subject to inappropriate conduct or are otherwise prevented from carrying out their responsibilities, we will carefully evaluate it to determine the proper course of action.