Before the Committee on Appropriations
Subcommittee on Transportation, Housing and Urban Development, and Related Agencies
United States Senate

For Release on Delivery
Expected at
2:30 p.m. EDT
Wednesday
March 16, 2016
CC-2016-007

Budget and Management Challenges Facing the Department of Transportation

Statement of
The Honorable Calvin L. Scovel III
Inspector General
U.S. Department of Transportation

Chairman Collins, Ranking Member Reed, and Members of the Subcommittee:

Thank you for inviting me here today to discuss the Department of Transportation's (DOT) budget priorities. Each year, the Department spends over $70 billion on a wide range of programs to meet its top priority of transportation safety and to maintain and modernize transportation systems. We remain committed to assisting DOT as it works to improve how it manages programs and resources. My statement today will focus on three cross-cutting management challenges: (1) addressing DOT's new and longstanding safety challenges, (2) continuing diligent stewardship over DOT's critical investments, and (3) enhancing DOT's information technology (IT) security and preparedness. Regardless of specific budget levels requested or approved, effective oversight and management of safety efforts, major transportation projects, and DOT assets are critical to ensure the greatest return on the taxpayers' investment.

SUMMARY

Safety is DOT's top priority, and the Department faces a range of emerging and longstanding safety challenges. These include safely integrating Unmanned Aircraft Systems (UAS) into the National Airspace System (NAS), addressing risks posed by the transport of hazardous materials (hazmat), and removing unsafe vehicles and commercial drivers from roadways. At the same time, DOT must carry out its safety mission within a framework of diligent stewardship over its investments and assets. In particular, continued attention to strengthening the Department's internal controls and risk-based oversight is critical to the efficiency of taxpayer-funded projects to build, repair, and maintain the Nation's surface transportation system. DOT can also do more to reduce risk in its billion-dollar efforts to modernize the Nation's aviation system and to develop and sustain a high-performing workforce. Finally, DOT continues to struggle to secure the 450-plus information systems it uses to conduct business and operate critical transportation systems, ensure continuity of operations, and safeguard systems from insider threats.

ADDRESSING NEW AND LONGSTANDING SAFETY CHALLENGES

Making the Nation's airspace, environment, and roads safer continues to be DOT's top priority. Addressing a number of new and longstanding safety issues we have identified will be critical for DOT to maintain and improve the Nation's transportation safety record. In addition to the new challenges of safely integrating UAS into the NAS, DOT must continue to reduce safety risks in transporting hazardous materials while improving safety on our Nation's roadways.

Integrating Unmanned Aircraft Systems Safely Into the National Airspace System

DOT, the Federal Aviation Administration (FAA), and industry have maintained a remarkably 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 precision agriculture operations to package delivery—presents one of the most significant safety challenges for FAA in decades. Analysts predict that as much as $93 billion will be invested in the technology worldwide over the next 10 years.

The FAA Modernization and Reform Act of 2012 requires FAA to take multiple steps to safely integrate UAS into the NAS. However, FAA and industry have not reached consensus on UAS-specific technology standards that are critical to safe integration. For example, FAA and industry still lack standards to ensure that UAS can automatically detect and successfully maneuver around other aircraft operating in nearby airspace.[1]

FAA also lacks a regulatory framework for UAS integration, which would govern areas such as small UAS (under 55 pounds) operations, beyond-line-of-sight procedures, larger unmanned aircraft systems, and pilot qualifications. FAA currently approves commercial UAS operations only on a case-by-case basis, leveraging an authority granted by Congress to exempt small UAS from certification requirements.[2] So far, FAA has issued over 3,800 exemptions. We are currently reviewing the UAS exemption and safety oversight processes. FAA intends to issue its rule on small UAS operations in late spring 2016—more than a year and a half behind the schedule established in the act. However, several high-profile aspects of UAS use—such as package delivery—will not be covered under the rule, which underscores the need for further regulatory efforts. FAA also has not established standard procedures for safely managing UAS in the same airspace as manned aircraft or an adequate UAS training program for controllers.

As the number of UAS operations continues to grow, safety and oversight will remain a significant concern. According to FAA, reported UAS sightings by pilots have increased significantly, with more than 1,100 reports in 2015, compared to just 238 reported in all of 2014. Some reports indicated safety risks, such as pilots altering the course of their aircraft to avoid UAS. Despite these risks, FAA does not have a formal system to track and classify the severity of UAS incidents. In addition, FAA inspectors still lack clear guidance on how to conduct UAS oversight. FAA reports that, through its recently established registration process, nearly 370,000 operators

[1] While FAA 14 CFR 91.113 describes a pilot's ability to "see and avoid" other aircraft, the UAS community is using the term "detect and avoid" to describe the desired capability of UAS.

[2] These requirements include the steps necessary to obtain an airworthiness certificate, including demonstrating to FAA that the UAS conforms to an approved aircraft design and is in condition for safe operation.

have already registered their unmanned aircraft. The impending rule on small UAS is likely to further increase the number of UAS in our airspace, making UAS oversight an increasingly critical responsibility for FAA's safety inspector workforce.

Strengthening Cross-Modal Efforts To Address Pipeline and Hazmat Safety Risks

A key DOT mission requiring strong cross-modal efforts is mitigating the safety risks posed by transportation of hazmat. From 2010 through 2014, there were more than 3,000 pipeline and 78,000 hazmat incidents in the United States, including about 3,500 rail incidents involving hazmat. These incidents resulted in fatalities and injuries, as well as environmental and property damage. Transportation of hazmat by air also presents serious risks, with more than 70 incidents worldwide between 1991 and 2014 involving lithium batteries in aviation cargo and passenger baggage.[3]

The Pipeline and Hazardous Materials Safety Administration (PHMSA) works to implement robust and timely safety measures for mitigating significant hazmat and pipeline accidents. However, PHMSA has made limited progress towards meeting safety recommendations by the National Transportation Safety Board (NTSB) and congressional mandates. For example, PHMSA has not fully implemented a 2007 NTSB recommendation to require railroads to immediately provide emergency responders with real-time information regarding the identity and location of all hazardous materials on a train. PHMSA also has not fully implemented the safety measures included in the Pipeline Safety, Regulatory Certainty, and Job Creation Act of 2011.[4] These measures aim to improve operators' assessments of gas pipelines, require leak detection systems on hazardous liquid pipelines, and establish regulations for transporting carbon dioxide by pipeline.

On the aviation front, FAA established the Hazardous Materials Voluntary Disclosure Reporting Program (HM VDRP) in 2006, which allows air carriers to voluntarily disclose violations of hazmat regulations without receiving civil penalties. While this is a good step towards encouraging air carriers to improve hazmat safety, our 2015 report[5] found that FAA lacked an adequate framework of internal controls to effectively carry out HM VDRP. For example, FAA requires air carriers to complete corrective actions for violations they disclose through the program. However, for 31 of the 48 (65 percent) closed cases we reviewed, FAA did not request sufficient evidence to verify that air carriers completed all corrective actions or conducted self-audits as required. In response to our findings, FAA recently issued a new policy to require air carriers to document all corrective actions taken and FAA regions to coordinate with FAA Headquarters on proposed corrective actions and significant HM

[3] These incidents included extreme heat, smoke, fire, or explosions in aviation cargo and passenger baggage.
[4] Public Law No. 112-90 (2012).
[5] *Program and Data Limitations Impede the Effectiveness of FAA's Hazardous Materials Voluntary Disclosure Reporting Program* (OIG Report Number AV-2015-034), March 13, 2015.

VDRP cases. Effective implementation of this policy will require follow through with adequate training and guidance to maximize HM VDRP's potential as a safety program.

Finally, the Federal Railroad Administration's (FRA) enforcement of PHMSA regulations plays a large role in the safety of hazmat transported by rail. In fiscal year 2015, FRA reported that its inspectors identified 1,670 violations of hazardous materials regulations, and the Agency fined railroads and other regulated entities[6] roughly $3.9 million. Key elements in an effective enforcement program are considering risk when allocating enforcement resources and imposing sufficient penalties to deter future violations. Last month, we issued a report identifying shortcomings in the risk assessments FRA uses for allocating hazardous materials inspection resources and raised concerns about FRA's use of civil penalties and lack of criminal case referrals to OIG. FRA has agreed to implement our recommended improvements.[7]

Increasing Safety on Our Nation's Highways

Recent large-scale recalls from automotive manufacturers and continued efforts to enforce motor carrier regulations highlight a number of safety challenges the Department faces. Over the last 2 years, General Motors (GM) has recalled nearly 9 million U.S. vehicles for a defect involving a faulty ignition switch after it received more than 100 reports of death claims and more than 200 injury claims.[8] The GM recall and others have prompted reviews and recommendations on how NHTSA can improve its safety processes and controls, and NHTSA is working to address these concerns. For example, in 2011 we made recommendations to strengthen NHTSA's Office of Defects Investigations' (ODI) procedures for documenting and retaining evidence on defects investigations, coordinating with foreign nations to identify safety defects or recalls, and documenting its justifications for not investigating identified defects. Last month, we reported on NHTSA's progress towards those recommendations.[9] While NHTSA has completed the agreed-upon actions, we are concerned with how it is implementing some of them; in particular, NHTSA lacks mechanisms to ensure staff consistently apply the new policies. For example in response to one of our recommendations, ODI agreed to document justifications for exceeding investigation timeliness goals; however, over 70 percent of delayed investigations we reviewed did not include justifications for why these goals were not met. We made two new recommendations to enhance ODI's quality control mechanisms, and NHTSA fully concurred.

[6] Entities that received these violations and fines may include railroads, shippers, or tank car repair facilities.

[7] *FRA's Oversight of Hazardous Materials Shipments Lacks Comprehensive Risk Evaluation and Focus on Deterrence* (OIG Report Number ST-2016-020), February 24, 2016.

[8] GM's ignition switch compensation fund had approved 124 death and 275 injury claims as of August 21, 2015.

[9] *Additional Efforts Are Needed To Ensure NHTSA's Full Implementation of OIG's 2011 Recommendations* (OIG Report Number ST-2016-021), February 24, 2016.

NHTSA also agreed to implement the 17 recommendations stemming from our June 2015 audit, which found weaknesses with how ODI collects vehicle safety data and uses that data to determine whether to open an investigation.[10] For example, ODI's processes were insufficient for verifying that manufacturers submit complete and accurate early warning reporting data, which can be essential for identifying potential safety trends or concerns.

It will also be critical for NHTSA to follow through on *NHTSA's Path Forward*, a 2015 self-evaluation report released by the Secretary of Transportation. Through this effort, the Secretary seeks to improve NHTSA's ability to hold manufacturers accountable by implementing more effective methods for overseeing carmakers and their suppliers, as well as collecting and communicating vital safety information. The Secretary also announced the formation of an expert panel to help strengthen NHTSA's defect investigation workforce. It will be important for DOT to closely monitor how NHTSA addresses the panel's findings and recommendations.

At the same time, DOT has important opportunities to improve the safety of its highway infrastructure, particularly the bridges and tunnels that connect our Nation's roadways. For example, the Federal Highway Administration (FHWA) must maintain momentum in its initiatives in response to our recommendations to implement data driven, risk-based oversight of bridges and implement improvements to bridge safety mandated under the Moving Ahead for Progress in the 21st Century Act (MAP-21).[11] FHWA must also continue its oversight of highway tunnel safety according to the National Tunnel Inspection Standards that became effective in August 2015 and maintain a national tunnel inventory.

Another critical—and longstanding—highway safety concern is reducing motor carrier fatalities. Our safety investigations continue to identify challenges for the Department and the Federal Motor Carrier Safety Administration (FMCSA) as they seek to remove unsafe motor carriers from highways. Since fiscal year 2008, we have opened 272 criminal investigations involving motor carrier safety. I would like to highlight two focus areas where the Department and FMCSA can bolster their safety efforts.

First, FMCSA must take stringent enforcement and out-of-service actions to remove motor carriers that repeatedly violate and blatantly seek to circumvent safety regulations, including (1) hours of service regulations and records of duty status; (2) medical, drug, and alcohol testing requirements for drivers; and (3) vehicle inspection, repair, and maintenance records. In some instances, these carriers have

[10] *Inadequate Data and Analysis Undermine NHTSA's Efforts To Identify and Investigate Vehicle Safety Concerns* (OIG Report Number ST-2015-063), June 18, 2015.
[11] *FHWA Has Not Fully Implemented All MAP-21 Bridge Provisions and Recommendations* (OIG Report Number MH-2014-089) August 21, 2014, and *FHWA Effectively Oversees Bridge Safety, but Opportunities Exist To Enhance Guidance and Address National Risks* (OIG Report Number ST-2015-027) February 18, 2015.

been involved in multi-vehicle crashes and fatalities. While FMCSA has taken enforcement actions and is collaborating with our office and other law enforcement partners to remove these carriers from service, carriers intent on breaking the law continue to pose a significant threat to highway safety. Key actions to keep unsafe carriers off the road include effective vetting of carriers' applications, focusing resources on high-risk carriers, and prosecuting companies that are caught violating the law.

The second area concerns reincarnated carriers—carriers that attempt to operate as different entities in order to evade FMCSA's enforcement actions. Reincarnated carriers have been involved in approximately 14 percent of the motor carrier safety investigations we opened since fiscal year 2008. For example, in Texas, we investigated a company that was issued an unsatisfactory safety rating by FMCSA for numerous violations, including falsifying hours-of-service requirements and using drivers who were not medically examined or certified. After being placed out of service by FMCSA, the company reincarnated under a different name and was involved in a passenger bus crash that killed 14 people. FMCSA proposed that Congress modify Section 521 of Title 49 U.S.C. to make it a criminal penalty for knowingly and willfully violating an out-of-service order, which will assist in prosecuting reincarnated carriers. Criminal penalties under Section 521 currently contain only a misdemeanor provision, which is difficult to prosecute and less likely to result in jail time if prosecuted; therefore, its effect as a deterrent is limited.[12]

CONTINUING DILIGENT STEWARDSHIP OVER DOT'S CRITICAL INVESTMENTS

Diligent stewardship of DOT's investments of taxpayer funds is vital for the Department to effectively carry out its mission. While DOT remains committed to strengthening its oversight for highway, rail, and transit projects, opportunities remain to improve its risk-based oversight of projects and strengthen financial controls to protect its investments. In addition, FAA faces challenges in its efforts to provide effective contract and acquisition management—a critical element in reducing risk for the major programs and systems in which it has invested.

Maximizing Federal Investments Through Improved Risk-Based Oversight and Better Financial Controls

DOT receives over $50 billion in Federal dollars annually to fund projects to build, repair, and maintain the Nation's surface transportation system. Strong risk-based oversight and financial controls are key to the success of the more than 100,000 transportation projects funded by the Federal Highway Administration (FHWA) and Federal Transit Administration (FTA) each year.

[12] 49 United States Code Section 521(b)(6)(A) is a misdemeanor statute for violations of certain FMCSA regulations.

FHWA recently revised its overall risk-based strategy to overseeing Federal-aid highway project funds. This revised effort includes improving the linkage between FHWA's annual assessments of State and Federal-aid highway programs and analyzing that information to better target its oversight reviews of highway and bridge projects. FHWA recently completed its first full performance cycle with these revised initiatives; in future performance cycles, management will need to assess whether the program is robust and working as designed and make improvements where needed.

However, to address more specific risks, FHWA needs to improve oversight of financial and program plans covering major highway and bridge projects—those exceeding $500 million in funding—to implement its new guidance on project estimating, and address the backlog of pending Federal-aid highway project closeouts to ensure effective use of Federal funds. In addition, FHWA has yet to finalize improvements to its financial information system to improve project data used to oversee its programs.

FTA has similar opportunities to better target its oversight and use tools to meet its goals to ensure major projects are on time and within budget. For example, FTA did not verify the adequacy of the Metropolitan Washington Airports Authority's (MWAA) support for claimed costs on grant expenses for FTA's Dulles Rail Project.[13] As a result, FTA initially reimbursed MWAA for more than $36 million in unsupported and unallowable costs.[14] In addition, FTA faces challenges in overseeing how local transportation agencies continue to use the approximately $10 billion in relief funds for Hurricane Sandy. In 2015, we reported that FTA had not fully implemented the processes and internal controls (required by the Disaster Relief Appropriations Act) it established to award and monitor Hurricane Sandy funds.[15] FTA also has yet to develop a formal coordination process with the Federal Emergency Management Agency to reduce the risk of duplicating emergency and disaster-related assistance.

Fraud remains another ongoing concern. For example, our investigators determined that an owner of a Massachusetts transit authority bus operator diverted grant funds that were designated to pay salaries, benefits, and other expenses for employees of the bus company.[16] Similarly, during liaison and coordination efforts with FTA and other

[13] *MWAA's Financial Management Controls Are Not Sufficient To Ensure Eligibility of Expenses on FTA's Dulles Rail Project Grant*, (OIG Report Number ZA-2014-021), January 16, 2014.

[14] FTA and Federal grant conditions require that grant recipients maintain support for federally funded project costs. MWAA did not have sufficient documentation to support some of the expenses charged to the Dulles Rail Project and these costs are considered unsupported. These principles also specify the types of costs that are allowable under Federal grant awards. An example of an unsupported cost that we found was invoices that said "labor" with no further details or documentation about what these charges included. An example of an unallowable cost that we found was $54,000 for expenses that were outside the scope of the Phase 1 Project to which they were charged.

[15] *FTA Has Not Fully Implemented Key Internal Controls for Hurricane Sandy Oversight and Future Emergency Relief Efforts* (OIG Report Number ST-2015-046), June 12, 2015.

[16] The former owner was sentenced in July 2015 to 70 months in prison and ordered to pay $688,772 in restitution in connection with his diversion of grant funds.

stakeholders, we discovered that a Hurricane Sandy grantee was not reporting fraud settlements to FTA. We have reported that the use of integrity monitors can help to prevent and detect fraud and noted the importance of sharing fraud allegations across organizations so we can partner to combat wrongdoing.[17] As we stated in June 2015,[18] FTA must focus on promptly addressing identified oversight issues; strengthening stakeholder agreements; and enhancing controls to prevent, detect, and report fraud.

Structuring Major Aviation Acquisitions To Successfully Manage Risk

FAA continues to award high-dollar contracts without fully addressing and mitigating risk in the acquisition planning and contract award stages, often resulting in large cost overruns and delays in system implementation.

First, FAA has had ongoing challenges in effectively structuring several of its major acquisitions.[19] These issues have been prevalent with the $1.8 billion Automatic Dependent Surveillance-Broadcast (ADS-B) system. ADS-B is a new satellite-based surveillance system for managing air traffic that is critical to the success of FAA's Next Generation Air Transportation System (NextGen). Since 2010, we have reported that FAA faces significant risks in implementing ADS-B and realizing benefits due to weaknesses such as its contract structure and oversight. For example, the ADS-B contract structure bundles tasks and costs, making it difficult for decisionmakers to manage the contract and track costs. In addition, FAA covered the first 18 years of ADS-B's 28-year lifecycle through one contract award, rather than breaking it into more manageable segments as OMB and the Federal Chief Information Officer recommend.[20] While FAA has finished deploying the 634 ADS-B ground radio stations, based on our ongoing review, it remains unclear whether FAA has fully mitigated past problems associated with contract management and oversight to ensure it can achieve ADS-B technical requirements and do so within budget. We plan to issue our next report providing an update on how FAA is addressing ADS-B contract weaknesses later this year.

Second, FAA did not take sufficient steps to assess and mitigate risk factors we identified on a previous significant contract when selecting a bidder and awarding the new contract, potentially resulting in increased costs to the Agency. In 2015, FAA decided to award a $727 million new Controller Training Contract (CTC), without

[17] *Initial Assessment of FTA's Oversight of the Emergency Relief Program and Hurricane Sandy Relief Funds* (OIG Report Number MH-2014-008), December 3, 2013.

[18] *Oversight of Major Transportation Projects: Opportunities To Apply Lessons Learned* (OIG Briefing No. CC-2015-010), June 8, 2015. We briefed Members of the Committee on Oversight and Government Reform, Subcommittee on Transportation and Public Assets, United States House of Representatives.

[19] These acquisitions include the Wide Area Augmentation System (WAAS) Program, the Standard Terminal Automation Replacement System (STARS), and the En Route Automation Modernization (ERAM) system. FAA has awarded contracts for these large modernization efforts using a grand design, rather than through successive incrementally priced awards--each of which experienced cost increases, delays, and performance issues.

[20] FAA's AMS lacks sufficient guidance on practices that could minimize mistakes associated with acquisition planning, such as using modular contracting to award information technology contracts in incremental, workable segments; and using contract line items, with separate pricing, contract types, and deliverables, to better manage the acquisition.

first addressing longstanding issues we reported with its prior controller training contract, the $859 million Air Traffic Control Optimum Training Solution (ATCOTS) contract. Specifically, in 2013, we reported that before awarding ATCOTS, FAA determined there was a 60- to 80-percent likelihood that the successful bidder would not meet FAA's training needs with the limited staff hours proposed.[21] However, FAA did not require the contractor to address this issue prior to award and had to spend millions of dollars more than expected to make up for the shortfall in contracted resources. We made 10 recommendations in 2013 to improve FAA's management and oversight of the ATCOTS contract. We recently reported that while FAA addressed recommendations related to contract administration practices and oversight, it has not implemented those related to better defining training requirements and validating training costs.[22] These recommendations were designed to improve FAA's ability to develop a comprehensive understanding of its training needs and, in turn, a more reliable estimate of the Agency's training costs. Because FAA awarded CTC without fully addressing these recommendations, it may encounter many of the same issues that compromised the success of the ATCOTS contract.

Developing and Sustaining an Effective and Skilled DOT Workforce

Maintaining an effective and skilled workforce is critical to ensuring a safe and vibrant transportation system. This means identifying and hiring the right number of staff with the requisite skill mix; adapting hiring and training practices to account for changing missions, requirements, and workforce demographics; and implementing policies and procedures that promote employees' success and ability to carry out DOT's mission effectively.

However, DOT agencies have not always taken adequate actions to ensure a robust workforce. For example, FAA lacks a comprehensive process for determining staffing levels needed to oversee its Organization Designation Authorization (ODA) program—a program that allows FAA to delegate certain functions, such as certifying aircraft components, to manufacturers and other organizations. Although FAA uses a staffing model to help identify overall ODA staffing needs, the model does not include detailed data on important workload drivers, such as a company's size and location, type of work performed, past performance, and project complexity and volume. In addition, FAA does not have the data or an effective model to accurately identify how many air traffic controllers it needs to maintain efficiency without compromising safety. Therefore, as we recently reported, many of FAA's busiest and most complex air traffic control facilities have a shortage of fully trained controllers.[23]

[21] *FAA Needs To Improve ATCOTS Contract Management To Achieve Its Air Traffic Controller Training Goals,* (OIG Report Number ZA-2014-018) December 18, 2013.
[22] *FAA Has Not Sufficiently Addressed Key Weaknesses Related to Its ATCOTS Contract* (OIG Report Number ZA-2016-010), December 10, 2015.
[23] *FAA Continues to Face Challenges in Ensuring Enough Fully Trained Controllers at Critical Facilities,* (OIG Report Number AV-2016-014), January 11, 2016.

We have an ongoing audit to examine FAA's new controller hiring process and the changes that have occurred since its implementation in 2014.

My office has made a number of recommendations to help DOT ensure its employees keep abreast of changing technology and missions. Now, agencies must follow through on actions planned in response to these recommendations. For example, in 2011 we found that NHTSA's ODI did not have a formal training program to help develop its current and future workforce to promote continuity of institutional knowledge. In 2015, NHTSA provided us a workforce assessment that evaluated its staffing and training needs for ODI. NHTSA must now fully implement the results of the workforce assessment to help inform future decisions on the resources required for this critical mission. Similarly, we found in 2014 that FHWA had not conducted a comprehensive assessment of MAP-21's impact on its workforce—despite the significant structural changes the act brought about, such as consolidation of several FHWA programs. FHWA has since completed an assessment that recognizes the Agency's need to make changes to the way it does business and deploys staff to meet MAP-21 requirements and carry out its mission effectively.

Changes in workforce demographics also present unique challenges for DOT. For example, 22 percent of DOT's acquisition workforce was retirement-eligible in fiscal year 2015, heightening the need for improved compliance with contracting officer (CO) training and experience requirements across all DOT agencies.[24] DOT's acquisition workforce is composed of hundreds of COs, CO representatives, and other supporting staff who provide agencies with the goods and services required to accomplish their mission at the best value to taxpayers.[25] While DOT has several training improvement initiatives under way for its acquisition workforce, our 2015 review found that it still needs to clarify and enforce its policies governing certification and warrant authority for COs.[26] Of the 63 COs we reviewed, 15 (24 percent) did not fully comply with DOT requirements. For example, 10 COs' certifications had expired, yet they continued to approve over 3,000 contract actions and obligate over $731 million. While DOT recently revised its acquisition workforce policy in response to our report, full implementation of our recommendations and enforcement of these policies will be critical to ensure that COs have the appropriate

[24] FAA is excluded from these data and the scope of our work described in this paragraph because Congress exempted FAA from Federal acquisition laws and regulations in DOT's fiscal year 1996 Appropriations Act. Congress provided FAA with broad authority to develop its own acquisition process. Under this authority, FAA developed the Acquisition Management System and a set of policies and guidance designed to address the unique needs of the Agency.

[25] COs are Government employees who can bind the Federal Government to a contract. COs are responsible for ensuring performance of all necessary actions for effective contracting, ensuring compliance with the terms of the contract, and safeguarding the interests of the United States in its contractual relationships. Contracting Officer Representatives (COR) are Government employees responsible for monitoring the contractor's progress in fulfilling the technical requirements specified in the contract. For example, CORs maintain administration records, approve invoices and perform quarterly monitoring reports to confirm the contractor is meeting the terms and conditions under the contract.

[26] *Some Deficiencies Exist in DOT's Enforcement and Oversight of Certification and Warrant Authority for Its Contracting Officers* (OIG Report Number ZA-2015-041), April 9, 2015.

training, experience, and certification to award and administer DOT's complex, high-dollar acquisitions.

ENHANCING DOT'S IT SECURITY AND PREPAREDNESS

Attacks on public and private sector information systems, carried out by increasingly well-funded and organized hackers, pose a continuous threat to the more than 450 information systems DOT uses to conduct business and operate some of the Nation's most critical transportation systems. While DOT has made progress in protecting its information systems, many remain vulnerable to compromise, underscoring the need for more effective contingency planning, and aggressive deterrence of insider threats.

Protecting DOT's Information Systems From Increasing Threats

DOT continues to face longstanding cybersecurity vulnerabilities and must take corrective actions to address identified weaknesses that pose threats to its information systems. To its credit, DOT has made major progress in implementing the required use of Personal Identification Verification (PIV) cards[27] for all DOT employees and contractors—a key step in securing access to DOT facilities and systems. DOT reported issuing PIV cards to 100 percent of its employees, and 98.3 percent have been configured for use in accessing networks—an increase of 74.5 percent from last year.

However, DOT has been slow to take corrective actions to address many other cybersecurity weaknesses. To help reduce cybersecurity risks, OMB requires agencies to track identified weaknesses using plans of actions and milestones (POA&M). Yet, in 2015, DOT had a backlog of more than 3,800 POA&Ms, which included 21 unimplemented recommendations we have made. DOT also remains behind schedule in implementing recommendations we have made in our annual Federal Information Security Management Act (FISMA) reports and other IT-related audits.

Many of our recommendations focus on key Administration priorities. For example, OMB requires agencies to implement continuous information system monitoring, which can provide near real-time security information to senior leaders, by 2017.[28]

[27] A PIV card is a smart card that contains the necessary data for the holder to be granted access to Federal facilities and information systems and assure appropriate levels of security for all applicable applications.

[28] Continuous monitoring involves establishing processes and capabilities to provide near real-time security information to senior leaders.

However, DOT has not yet defined the practices or technologies that should be used or established common security controls[29] to help protect its information systems, including high-value asset[30] systems. Specifically, DOT is still conducting planning and research to determine the resources needed to ensure that common controls are properly used, implemented, and monitored. Until those are finalized, DOT remains vulnerable to more aggressive and complex cyber threats due to insufficient security controls.

Strengthening Contingency Plans and Security Protocols To Deter Insider Threats

We continue to find weaknesses in DOT's ability to plan for contingencies and recover from disruptions, even for critical systems. For example, our ongoing work has shown that several Operating Administrations did not conduct annual contingency plan testing for their selected mission critical or high- and moderate-impact systems to ensure they will work in the event of a disruption, as required.[31] Specifically, 5 of the Department's 12 Operating Administrations did not comply with DOT policy to conduct such testing or meet all DOT requirements for their disaster recovery plans, potentially limiting their effectiveness at ensuring continuity of critical systems in the event of a malicious attack.

The importance of effective contingency plans was demonstrated on September 26, 2014, when an FAA contract employee deliberately started a fire that destroyed critical telecommunications equipment at FAA's Chicago Air Route Traffic Control Center in Aurora, IL. As a result of the damage, Chicago Center was unable to control air traffic for more than 2 weeks,[32] thousands of flights were delayed or cancelled, and aviation stakeholders and airlines reportedly lost over $350 million. While FAA completed comprehensive reviews of its contingency plans and security procedures following the Chicago Center incident, significant work remains to prevent or mitigate the impact of similar events in the future.

Notably, the event highlighted the need to enhance security and increase the flexibility and resiliency of the national air traffic control system. For example, FAA lacked the controls necessary to block access to a contract employee no longer assigned to this facility, thereby leaving the Center's high-value systems vulnerable to

[29] Necessary to meet requirements of the National Institute of Standards and Technology (NIST), common system security controls are controls that exist in one system that can be used to protect other systems.

[30] High-value assets are assets, systems, or datasets that may be considered "high-value" by the Department based on the following attributes—sensitivity of the information, uniqueness of the dataset, impact of loss or compromise, system dependencies, and systems that are integral to supporting critical department communications. A system is considered "high impact" if the loss of confidentiality, integrity, or availability for that system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

[31] Departmental Cybersecurity Compendium Supplement to DOT Order 1351.37, "Departmental Cybersecurity Policy," Version 3.0, September 2013.

[32] Chicago Center's air traffic and airspace responsibilities were eventually transferred to other facilities, based on a 2008 contingency plan and airspace map. This required extensive adjustments to ensure adequate radar and radio communication coverage.

unauthorized access, disruption, and loss of information. Other insider threats pose significant threats to security, ranging from an employee who maliciously steals data to an employee who unwittingly opens infected email attachments. For example, in 2014, a DOT employee opened an infected email attachment and unleashed a serious computer virus (known as "Dyre") into DOT's network, compromising more than 5,000 computers and resulting in loss of productivity, email interruptions, and data loss. The virus was designed to steal information (including passwords), avoid routine detection, and generate new emails with attachments to further spread the virus. While DOT reported that the virus has been mostly eradicated, it noted the need to better train employees to protect DOT's systems to lower the risk of system compromise.

CONCLUSION

The safe and efficient movement of people and goods is vital to our Nation's economic growth, global partnerships, and quality of life. The Department has clearly demonstrated its commitment to advance these priorities. To continue addressing the management issues we have identified as well as a changing transportation environment, it will be important for the Department to follow through with new safety standards and recommended actions, stronger financial and project controls over major investments, and vigilant security and preparedness measures.

We remain committed to assisting DOT as it works to improve how it manages programs and resources and to our role in ensuring the greatest return on investment to taxpayers. I appreciate this Committee's continued support in the coming fiscal year to enable us to enhance our coverage of the Department's safety programs, high-dollar administrative and management assets, and information systems security.

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