Office of Inspector General

Audit Report

DOT CYBERSECURITY INCIDENT HANDLING AND REPORTING IS INEFFECTIVE AND INCOMPLETE

The Department of Transportation

Report Number: FI-2017-001

Date Issued: October 13, 2016

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: **ACTION:** DOT Cybersecurity Incident Handling and Reporting is Ineffective and Incomplete Department of Transportation Report No. FI-2017-001

Date: October 13, 2016

From: Louis C. King
Assistant Inspector General
for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: Chief Information Officer, DOT
Chief Information Officer, FAA

The number of cyber incidents reported by Federal agencies has increased significantly over the last several years. For example, in 2014, the Department of Transportation (DOT) experienced over 2,200 incidents that affected its operations. These incidents have also increased in breadth and depth throughout the Federal Government. In June 2015, the Office of Personnel Management reported that two intrusions alone were so large that they had possibly compromised the information of approximately 22 million current and former Federal employees and contractors.

An effective response to cyber incidents minimizes disruptions to information systems and data losses. We self-initiated this audit because of DOT's large number of information systems that contain sensitive data. Our audit objective was to determine whether DOT has effective cyber security monitoring in place for its networks and information systems. Specifically, we assessed DOT's policies and procedures for (1) monitoring, detecting, and eradicating cyber incidents, and (2) reporting incidents and their resolutions to appropriate authorities.

We conducted our work in accordance with generally accepted Government auditing standards. We reviewed policy documentation, including the Department's Cyber Security Incident Response Plan (IRP).[1] We interviewed

[1] DOT Office of the Chief Information Officer Cyber Security Incident Response Plan, March 2014.

personnel in the Office of the Chief Information Officer (OCIO), personnel at the Federal Aviation Administration's (FAA) Air Traffic Organization, subject matter experts at the Cyber Security Management Center's (CSMC) Security Operations Center, and staff at FAA's National Airspace System's (NAS) Cyber Operations (NCO) and DOT's Common Operating Environment (COE). During these interviews, we were briefed on the processes for detecting and handling incidents. See exhibit A for additional details on our scope and methodology.

RESULTS IN BRIEF

OCIO has not ensured that the Security Operations Center (Center) has access to all departmental systems or required the Center to consider incident risk, thus limiting the Center's ability to effectively monitor, detect, and eradicate cyber incidents throughout the Department. Federal law requires agency heads to ensure that their information and information systems are secure, and to delegate to their chief information officers the authority to ensure compliance with Federal requirements. However, OCIO does not enforce Federal and departmental policy that requires all Operating Administrations (OA) to give the Center access to their systems for incident monitoring. OCIO officials attributed this to the unique authorities and relationships that exist between FAA and OCIO. Yet, this does not explain the lack of enforcement of cyber security policies. We also found that without OCIO's approval, FAA conducts its own monitoring of the NAS[2] through NCO, and this monitoring is incomplete. FAA officials have identified 39 NAS systems to be monitored but have initiated monitoring of only 11. Furthermore, OCIO has not ensured that the OAs that have cloud systems require their contracted cloud services providers to allow the Center to monitor the systems. OCIO's lack of enforcement of DOT's cyber security policies coupled with the weaknesses in FAA's monitoring puts the Department's information systems at risk for compromise. OCIO also has not ensured that the Center has implemented a ranking scheme for incidents based on the seriousness of the risk they pose, and as a result, the OAs do not have the information they need to prioritize their incident responses. Consequently, OCIO cannot be sure that the OAs address the most serious incidents promptly. Furthermore, OCIO has not ensured that the OAs provide their network maps[3] to the Center. According to an OCIO official, the

[2] The NAS controls air travel within the United States and its systems provide services such as air traffic control, weather information, and status of airport facilities, including runways to commercial airlines and privately operating aircraft.

[3] DOT's policy requires that system owners develop and maintain the mapping of all devices in their networks, including identification of assets, network components, internet protocol addresses, and interconnections and/or interfaces to other systems. For infrastructure-type systems, these maps include those needed for both network operations and support, and the owners' system-level security responsibilities. DOT's incident response plan requires the OAs to provide this information to CSMC.

OAs do not provide the maps despite direction to do so. Consequently, the Center cannot determine which system an incident has affected, and rate its priority.

Because OCIO does not ensure that the OAs provide the Center complete system access, the Center's reports to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) and OIG are incomplete. The National Institute of Standards and Technology (NIST) requires departmental points of contact, such as the Center, to report to US-CERT in timely manner the type of each incident, such as malicious code and unauthorized access. DOT cybersecurity policy requires the Center to report to OIG for investigation incidents in which the amount of damage to the Department exceeds $5,000. FAA's policy also calls for reporting to the Center, but FAA officials stated that during our review period, the Agency did not identify any incidents to report. However, we found the following incidents in the NAS's systems that FAA should have reported: (1) a September 2014 fire at the Chicago air route traffic control center that affected NAS systems and flight operations; and (2) malware in maintenance data terminals connected to NAS systems. Lastly, the Center cannot report to US-CERT on departmental cloud systems because it does not monitor them. The Center's inability to monitor all departmental networks and devices increases the likelihood that security incidents will not be reported and mitigated. Incomplete reporting from agencies undermines US-CERT's and law enforcement's efforts to address serious incidents.

We are making recommendations to improve the effectiveness of DOT's cyber security incident handling and response.

BACKGROUND

OCIO serves as the principal advisor to the Secretary of Transportation on information and technology. The Department's CIO is responsible for overall cybersecurity incident management and response, mitigation, and recovery, including the oversight and enforcement of policies, standards, processes, and procedures. OCIO has also established departmental cybersecurity policy in the Cybersecurity Compendium.[4]

NIST Special Publication 800-61, Computer Security Incident Handling Guide,[5] defines a cybersecurity incident as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. According to the Department's IRP, CSMC's Center—under the leadership of

[4] DOT Cybersecurity Policy, Version 3.0, September 2013.
[5] NIST, August 2012.

DOT's and FAA's Chief Information Security Officers—is responsible for developing, managing, and enforcing DOT's cybersecurity incident response requirements.

The IRP also requires OAs to create maps, or up-to-date graphical representations, of their information networks that include the networks, systems, devices, and data. These maps help the OAs and the Department maintain up-to-date awareness of all IT assets and information.

NIST's SP 800-61 also requires each department to designate a point of contact for the Department of Homeland Security's United States-Computer Emergency Readiness Team (US-CERT). In the IRP, the Department designates CSMC's Center as its sole authority for communicating cybersecurity incidents to US-CERT and other Federal authorities responsible for incident management. The IRP also describes the OAs' responsibilities for reporting incidents to the Center on suspicious activities they detect such as lost and stolen information and assets.[6]

OCIO DOES NOT PROVIDE THE CENTER WITH APPROPRIATE ACCESS FOR MONITORING OR CONSIDER INCIDENT RISK

OCIO has not ensured that the Center has access to all departmental systems, including cloud systems, or that it considers incident risk. OCIO also has not ensured the Center has implemented a ranking scheme for incidents based on the seriousness of the risk they pose. Furthermore, the Center cannot identify the system on which an incident occurred because OCIO has not ensured the OAs provide their network maps.

Despite DOT Requirements, FAA Does Not Provide the Center with Access to Its NAS Systems

OCIO has not ensured that the Center has access to FAA's NAS systems. It does not require FAA to give the Center access to its NAS systems for monitoring as called for by DOT's Cyber Security Compendium.[7] In response to our request for an explanation of why OCIO does not enforce the Compendium's requirement, senior officials explained that unique authorities and relationships exist between FAA and OCIO. They explained further that responsibility for ensuring access cascades through the FAA Administrator to FAA senior leadership, with coordination at key points between OCIO and other functional areas as

[6] The OAs' reports to the Center on suspicious activities were outside the scope of our audit.
[7] The Compendium states that the OAs must ensure that the Center has full network visibility of all systems within their purview, including systems operated on their behalf by contractors and other Government organizations.

appropriate. However, these statements do not explain the lack of enforcement of the Compendium. Additionally, these officials stated further that DOT's departmental policy does not reflect this unique relationship. This lack of access to all departmental systems inhibits the Center's ability to perform its duties of developing, managing, and enforcing DOT's cybersecurity incident response requirements and as a result, puts the Department's systems at risk for compromise.

Furthermore, FAA, without consulting OCIO, has begun implementing a separate monitoring system for the NAS. In 2013, FAA gave responsibility to NCO for monitoring the NAS[8] for security incidents after highly publicized breaches of Federal systems resulted in new requirements from NIST. OCIO officials informed us that FAA did not consult them about its creation of NCO. In response to our questions about the separate monitoring, FAA officials stated that:

- The Center is not able to adequately monitor the NAS because elements of the NAS are industrial control systems[9] rather than IT systems—a condition, we note, that may exclude requirements for certain security controls;

- The NAS is an isolated network that communicates externally to customers via multiple monitored connections. These monitored connections provide protection to the NAS and ensure secure communication with other systems and networks. NCO and a contractor maintain control of the network by restricting system access to recognized partners and monitoring the information that flows through the entry points for cybersecurity; and

- Because the contractor identifies incidents in the NAS and resolves them at the entry points, the NAS is at low risk for compromise.

We found that this incident handling process for the NAS that FAA has set up in NCO is ineffective. Rather than the single controlled entry point that FAA described to us, the NAS's network includes a number of uncontrolled entry points in both NCO monitored and non-monitored systems that put the NAS's systems at risk for compromise. Specifically, 3 of the 11 systems that NCO [redacted]

[8] FAA Order 6000-15G (General Maintenance Handbook for NAS Facilities) gives responsibility to NCO for monitoring the NAS for security incidents.

[9] The term industrial control system describes several types of systems, including information systems, used by public and private sector entities in industrial production such as water treatment, nuclear power, and automobile manufacturing. They differ from IT systems in several ways, including no requirement for user identity authentication for system access, and a longer lifespan—15 to 20 years versus the 3 to 5 years of IT systems.

[redacted]—use unmonitored communications lines to connect to systems and equipment outside the NAS. Technicians use 1 of these 3 systems to maintain and make changes to 24 NAS systems, and consequently, this system provides uncontrolled access to all those systems. FAA first identified this system's use of an unmonitored communication line in a plan of action and milestone (POA&M)[11] established in 2006. The Agency began monitoring the system in 2014 but does not monitor the communication lines. Finally, FAA officials informed us that they had reclassified 39 NAS systems from industrial controls systems to IT systems, but have incorporated only 11 of these 39 into NCO's monitoring program. FAA officials also informed us that they planned to add the remaining 28 systems as they become ready. During our audit, FAA developed a schedule for incorporating the 28 systems into NCO by the end of fiscal year 2018.

In addition to our concerns, others have identified issues impacting the NAS monitoring system. In a 2015 report,[12] the Government Accountability Office (GAO) identified significant security control weaknesses in NAS systems and networks, threatening FAA's ability to adequately fulfill its missions. The Center has also identified a high incidence of malware on maintenance terminals that FAA technicians use for non-NAS activities. FAA officials informed us that the terminals' configuration is based upon the Agency's mission requirements and that they accept the risk of this configuration. They also informed us that a planned operating system upgrade will improve malware protection.

OCIO Does Not Ensure that OAs Include Provisions for Monitoring in Contracts with Cloud Services Providers

OCIO has not ensured that OAs' contracts with cloud services providers include provisions on system monitoring. In 2015, we found that four OAs—the National Highway Traffic Safety Administration, the Federal Highway Administration, the Federal Railroad Administration, and the Office of the Secretary of Transportation—had cloud services contracts that did not contain provisions allowing the Center to monitor the cloud systems for cyber incidents.[13] DOT's IRP requires OAs to ensure that contracts for cloud services include provisions for security support and response to protect information integrity, availability, and

[redacted]

According to NIST SP 800.37, an agency must open a POA&M on every vulnerability that it detects in this system to plan its resolution for that vulnerability.

[12] GAO, *FAA Needs to Address Weaknesses in Air Traffic Control Systems*, GAO-15-221, January 2015.

[13] *DOT Lacks an Effective Process for Its Transition to Cloud Computing*, OIG Report Number FI-2015-047, June 16, 2015.

confidentiality. An OCIO official stated that the OAs have not established these contract provisions despite OCIO's instruction to do so. OCIO's lack of enforcement of DOT's cyber security policies coupled with the weaknesses in FAA's monitoring puts the Department's information systems at risk for compromise.

OCIO Has Not Ensured that the Center Has Implemented a Ranking Scheme for Prioritization of Incident Resolution

OCIO has not fully complied with the IRP and NIST guidelines by ensuring the Center implements a ranking scheme based on the seriousness of incident risk so that OAs can prioritize incident resolution. For the systems it monitors, the Center detects incidents and informs the affected OA of the actions it needs to take to resolve the incidents. Under the IRP, each OA is responsible for resolving the incidents in its systems. Between June 2014, and June 2015, the Center identified over 6200 incidents of possible security violations and informed the affected OAs of the actions they needed to take to resolve the incidents.

NIST's Special Publication 800-61 calls for departments to consider incidents' risk so they can prioritize responses based on the seriousness of the risk. However, the Center has not implemented a ranking scheme to apply to incidents that indicates the incidents' risk to the affected OA. The Center informs the affected OA that the incident has occurred and how to resolve it, but does not indicate the incident's possible impact. As a result of this lack of information, the OA may not have the appropriate information to decide whether to take immediate action to resolve the incident or to accept the incident's risk.

For incidents that it does not resolve immediately, DOT's Cybersecurity Compendium requires the OA to open a POA&M to resolve the incident in the future. However, we found that for 276 incidents that were not immediately resolved, the OAs developed only 3 POA&Ms.

In response to questions regarding why OCIO had not implemented a ranking scheme for prioritization of incident resolution, an OCIO official informed us that:

- The incident response position in the Chief Information Security Officer's office is currently vacant and the office is recruiting to fill the position;

- Due to other priorities and resource constraints, the Department has not provided sufficient training to the OAs to ensure that personnel have the knowledge they need to handle prioritized risks; and

- Some OAs do not sufficiently oversee their own incidents to ensure that the information they provide to the Center is complete.

Because of this lack of a ranking scheme, the OAs do not have the information they need to prioritize their incident responses, and consequently, OCIO cannot be sure that the OAs address the most serious incidents promptly.

OCIO Does Not Ensure that OAs Provide their Network Maps to the Center

OCIO does not enforce the IRP's requirement that the OAs provide their network maps to the Center. The maps would allow the Center to determine what system an incident has affected, and rate its priority. Without the maps, the Center cannot identify the system name or function, and can only provide the internet protocol (IP) address[14] at which an incident has occurred to the OA. An OCIO official informed us that the OAs are not providing the maps despite direction to do so. Because of this lack of information from the network maps, the OAs do not have the information they need to prioritize their incident responses.

THE CENTER'S INCIDENT REPORTING IS INCOMPLETE

The Center's lack of access to FAA's NAS systems and cloud systems contributes significantly to the Center's incomplete reporting to US-CERT and law enforcement. The Center reports to US-CERT and law enforcement according to NIST requirements on incidents it identifies on systems in the networks it monitors. However, it does not identify specific systems by name or type. NIST's SP 800-61 requires departmental points of contact to report the following to US-CERT:

- The description of the affected resources, including the system's name;
- The type of incident, such as malicious code and unauthorized access;
- In the time required, depending on the type of incident; and
- Additional information on specific malicious code that it is tracking, such as Dyre—a virus that harvests personal information from compromised computers.

[14] An IP address is a numerical label assigned to each device, such as a computer and a printer, connected to a network that uses the Internet Protocol for communication. The Internet Protocol, developed and updated by the Internet Engineering Task Force, is the standard for transmitting data over the Internet and provides about 4.3 billion addresses for use worldwide.

Under DOT's Cyber Security Compendium, the Center also must report to OIG for investigation incidents in which the amount of damage to the Department exceeds $5,000.

We found that the Center reported to US-CERT over 95 percent of the 6200 identified incidents of possible security violations. Most of the five percent that the Center did not report involved events that had been misidentified as security incidents. The Center does not report the specific systems affected by particular incidents because it does not have that information.

The Center does not report on FAA's NAS systems because OCIO does not require that FAA provide the Center access to these systems. As we discussed previously, senior OCIO officials explained the unique authorities and relationships between FAA and OCIO, but not FAA's lack of reporting to the Center on NAS systems, even though its NAS Information Security Policy[15] calls for NCO to report incidents to the Center. FAA has not reported any incidents to the Center in the systems that NCO monitors. FAA informed us that during the period of our review, it did not identify any incidents that NCO needed to report to the Center. Despite FAA's claim, we found that the following reportable incidents had occurred and were not reported:

- In September 2014, a contractor that did not have access authorization started a fire at the Chicago air route traffic control center that affected NAS systems and flight operations. Under FAA's definition of unauthorized access, NCO should have identified this incident and reported it to the Center. However, NCO did not identify this occurrence as a security incident and therefore did not report it to the Center. While FAA stated that this was not a cyber security incident, according to its NAS Information Security Incident Policy, the disruption of service and abuse of systems are reportable incidents.

- FAA's maintenance terminals connected to systems that the Center monitors—in which the Center has identified malware—are also connected to NAS systems that NCO monitors. However, NCO has not reported to the Center any incidents in these terminals. The Center reported to US-CERT the ones it detected.

NIST also calls for departments to report incidents in cloud systems to US-CERT within specified timeframes. In our 2015 review of cloud systems, we found that the Center cannot monitor cloud systems because OCIO had not required the OAs

[15] FAA, Notice 1370.101A, NAS Information Security Incident Detection, Reporting, and Response, September 2015.

to include provisions in their contracts with cloud services providers that give the Center access to these systems for monitoring.

As a result of its inability to monitor NAS and cloud systems due to its lack of access, the Center cannot report to US-CERT incidents that occur in the these systems. Furthermore the Department cannot be sure that all cyber security incidents are reported to US-CERT and law enforcement. Consequently, DOT and US-CERT cannot be sure that they are mitigating cyber incidents effectively.

CONCLUSION

The increasing dependency upon IT systems pervades nearly every aspect of society. While bringing significant benefits, this dependency also creates vulnerabilities to cyber-based threats. To mitigate such threats, agencies establish incident response plan to detect security incidents and properly report them to appropriate officials. Such reporting allows officials to prioritize and mitigate incidents. While it has established an incident handling and reporting process, OCIO cannot fully detect, prioritize, or report incidents. Until corrected, this lack of full oversight inhibits OCIO's ability to ensure DOT's compliance with critical Federal cybersecurity requirements.

RECOMMENDATIONS

To improve effectiveness of DOT's cyber security incident handling and response, we recommend that the DOT Chief Information Officer:

1. Enforce DOT's current policy for incident monitoring to ensure the Cyber Security Management Center's access to FAA's NAS systems and departmental cloud systems, or update the policy to reflect the unique reporting structures between DOT and FAA.

2. Establish policy and controls for the use of maintenance data terminals to reduce the incidence of malware on these terminals.

3. Implement a ranking method for incidents.

4. Require OAs to provide their network maps to the Cyber Security Management Center.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided the Department with a draft copy of this report on August 26, 2016, and received its response on September 26, 2016, which is included as an appendix to this report. DOT concurred with recommendations 1 through 3 and provided appropriate planned actions and completion dates. While DOT did not concur with recommendation 4 as written, the DOT CIO proposed alternative actions and a target action date that meet the intent of the recommendation. The alternative actions include making available to the Center the information it needs to analyze incidents for risk. We therefore consider recommendations 1 through 4 resolved but open pending completion of planned actions.

We appreciate the courtesies and cooperation of DOT and its OAs' representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-4350, or Abdil Salah, Program Director, at (202) 366-8543.

#

cc: DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-100

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted this audit between March 2015 and August 2016. We conducted our audit work in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit covered incident handling for information systems and networks within DOT's internal and external information system networks, including NCO and cloud service providers' systems reported in Cyber Security Asset Management system. It also supported and augmented OIG's fiscal year 2015 FISMA audit. Our audit objectives were to determine whether DOT has: effective cyber security monitoring in place for its networks and information systems; an effective process to detect cyber incidents affecting Agency systems; and established management practices that reasonably contain, eradicate and report those cyber incidents. Specifically, we assessed DOT's policies and procedures for: (1) monitoring for, detecting, and eradicating cyber incidents; and (2) reporting incidents and their resolutions to appropriate authorities.

To conduct our work, we reviewed DOT's IRP in conjunction with NIST special publications. We visited DOT's three major security operations center locations, and FAA and DOT Headquarters to review processes and operational effectiveness for evaluating cyber security incident handling and reporting. We obtained all incident data reported from the Center, FAA's Telecommunications Infrastructure (FTI) Security Operations Center,[16] and NCO for the period of June 1, 2014 through June 30, 2015.[17] We found that incident data retrieved via the Center's remote reporting application did not contain all the information available in the application. To ensure accuracy and completeness, we retrieved all the incidents directly from the application at each site. Therefore, we deemed the incident data sufficiently reliable for the purposes of our audit. We analyzed the incident reports to determine whether procedures were followed and incidents and threats were identified, responded to, and mitigated appropriately. Using incident

[16] Harris FTI Center, Melbourne, FL.
[17] The Department and OIG have established June 30 as the cutoff date for the FISMA reporting process.

ticket data, we also determined whether incidents were characterized according to US-CERT categories and met reporting response requirements.

To assess DOT's policies and procedures, we reviewed OCIO's IRP and the Department's Cybersecurity Compendium, NIST's special publications, and OMB's guidance. We performed assessments of DOT's monitoring, detection and response capabilities at the Center, and FAA's FTI Center and NCO. At each site, we discussed with personnel the roles and responsibilities for monitoring the systems and detecting, containing, eradicating, and reporting cyber incidents.

To support FISMA related audit areas, we linked our audit program with Department of Homeland Security's Cyber Scope[18] questions relating to incident response and reporting. We assessed DOT's network monitoring capability—including topology maps and information systems diagrams—to compare and analyze with tools to validate. We also assessed DOT's capabilities to identify the dynamic network boundaries to comply with DHS trusted internet connections. Finally, we reviewed the Department's ability to detect cyber incidents that could harm its assets and information systems, compromise information, or impact operations.

[18] DHS provides a template to review information technology processes and operations of incident response and handling and other critical security areas.

Exhibit A. Scope and Methodology

EXHIBIT B. ORGANIZATIONS VISITED OR CONTACTED

Department of Transportation Headquarters

- Office of the Chief Information Officer
- Office of the Secretary of Transportation Common Operating Environment

Federal Aviation Administration Headquarters

- Office of the Chief Information Officer
- Air Traffic Organization

Cyber Security Management Center, Leesburg, VA

FAA's FTI Security Operations Center, Melbourne, FL

FAA's NAS Cyber Operations, Warrenton, VA

EXHIBIT C. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Abdil Salah	Program Director
Severin Pefoubou	Project Manager
James Mullen	Information Technology Specialist
Shavon Moore	Information Technology Specialist
Susan Neill	Writer-Editor
Petra Swartzlander	Sr. Statistician
Fritz Swartzbaugh	Associate Counsel

APPENDIX. AGENCY COMMENTS

U.S. Department of Transportation
Office of the Secretary of Transportation

MEMORANDUM

Subject: **INFORMATION:** Management Comments – Office of Inspector General (OIG) Draft Report on Cybersecurity Incident Handling and Reporting

Date: September 26, 2016

From: Richard McKinney
DOT Chief Information Officer

RICHARD MCKINNEY
Digitally signed by RICHARD MCKINNEY
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=RICHARD MCKINNEY
Date: 2016.09.26 16:29:27 -04'00'

To: Louis C. King
Assistant Inspector General for
Financial and Information Technology Audits

We do not share the IG's assessment of the current effectiveness of DOT's program. Each year DOT responds to thousands of security incident reports, for the hundreds of systems in the DOT inventory, with no major incident or breach, and no significant impact to a DOT information system.

Cybersecurity incident detection, response, reporting, and recovery are core capabilities of a Federal cybersecurity incident response program. The maturity and effectiveness of these capabilities are part of the NIST Cybersecurity Framework, and the Office of Management and Budget measures performance as part of its oversight of agency programs. Accordingly, the DOT Chief Information Officer piloted the new US-CERT incident response reporting criteria in Fiscal Year (FY) 2015, and implemented the new scheme in the first quarter of FY 2016. The Department also began deployment of Federal Continuous Diagnostics and

Mitigation (CDM) capabilities in FY 2016, and conducted a network assessment in FY 2016.

Based upon our review of the draft report, we concur with the recommendations 1, 2 and 3 as written. Our target action date for completing these recommendations is October 1, 2017.

We do not concur with recommendation 4. We propose an alternative action to leverage DOT CDM and enterprise network management capabilities to ensure that the DOT Security Operations Center (SOC) has necessary information to identify assets and properly assess impacts. We also propose that Component ISSMs provide the required information. Our target to complete these actions is June 30, 2017.

We appreciate the opportunity to comment on OIG's draft report. If you have any questions or need clarifications, please feel free to contact Andrew Orndorff andrew.orndorff@dot.gov, 202-366-9201 or Sherri Ellis, sherri.ellis@dot.gov, 202-366-1471.

Appendix. Agency Comments