Office of Inspector General

Audit Report

CYBERSECURITY PLANNING WEAKNESSES MAY HINDER THE EFFICIENT USE OF FUTURE RESOURCES

Office of the Secretary

Report Number: FI2017066

Date Issued: August 7, 2017

Memorandum

U.S. Department of Transportation
Office of Inspector General

Subject: **ACTION**: Cybersecurity Planning Weaknesses May Hinder the Efficient Use of Future Resources
Office of the Secretary
Report No. FI2017066

Date: August 7, 2017

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

Reply to Attn. of: JA-20

To: Chief Information Officer

In its fiscal year 2011 budget request, the Department's Office of the Chief Information Officer (OCIO) requested a one-time appropriation of $30 million to close the Department's most serious cybersecurity[1] gaps. Between fiscal years 2012 through 2015, Congress appropriated almost $29 million to support DOT's cybersecurity initiatives. Persistent weaknesses—such as those described in our 2015 review[2] required by the Federal Information Security Management Act of 2002[3] (FISMA)—underscore the importance of the Department's use of available funds to the extent possible to secure its systems.

Due to the large investments that OCIO has made in cybersecurity over recent years, we initiated this audit. Our objectives were to determine whether OCIO (1) expended the appropriated funds to support cybersecurity initiatives, and (2) adequately planned for its cybersecurity funding needs.

We conducted this audit in accordance with generally accepted Government auditing standards. To conduct our work, we reviewed Office of the Secretary (OST) and congressional budget information, Office of Management and Budget (OMB) and DOT's budget guidance,[4] and Homeland Security Presidential Directives[5] that define cybersecurity priorities and initiatives. We also reviewed

[1] Cybersecurity is the process of protecting information by preventing, detecting and responding to attacks.

[2] *DOT Had Major Success in PIV Implementation, but Problems Persist in Other Cybersecurity Areas* (OIG Report No. FI2016001), November 5, 2015. OIG reports are available on our website: https://www.oig.dot.gov/.

[3] Public Law No. 107-347, Section 301 (2002).

[4] DOT Performance Budget Instructions for OST Submission for Fiscal Years 2013, 2014 and 2015.

[5] HSPD-12, *Policies for a Common Identification Standard for Federal Employees and Contractors*, February 2011; HSPD-23, *Cybersecurity Policy*, January 2008.

OCIO's budget planning documents, internal reports and studies, and interviewed DOT officials. See exhibit A for details on our scope and methodology.

RESULTS IN BRIEF

We did not find any instances where OCIO expended the $29 million in appropriated funds received between 2012 and 2015 on non-cybersecurity initiatives. At the time of our review, OCIO had approximately $23.4 million in expenditures out of the $29 million. We sampled 61 of 181 transactions with an expenditure amount of $18.26 million or 78.2 percent of the $23.4 million. All sampled transactions were in support of cybersecurity initiatives. However, OCIO did not consistently apply billing procedures when expending funds through the Working Capital Fund (WCF).[6] We found that $285,352 (7.65 percent) of the $3.73 million in cybersecurity funds advanced to and expended via the WCF was used to pay for services outside of the period of performance and scope of work outlined in OCIO cybersecurity funded intra-agency agreements. Such errors make it difficult for OCIO to ensure that WCF customers are accurately and consistently charged for services as described in customer agreements.

OCIO did not adequately document or plan for its cybersecurity funding needs. OCIO did not maintain adequate support documentation to justify its costs estimates for the amount of cybersecurity funds requested in budget years 2014, and 2015. Additionally, OCIO did not always follow OMB or its own acquisition planning guidance for three information technology (IT) projects that accounted for about $20 million (68 percent) of the $29 million appropriated. For example, OCIO did not provide evidence that it developed and documented alternative analyses for two of the three IT projects, or established realistic initial costs and schedule estimates. As a result, we could not assess the reasonableness of OCIO's costs for its IT projects. Lastly, while OCIO developed strategic plans outlining its long-term cybersecurity goals, it did not develop tactical plans to prioritize which IT projects OCIO would invest in, raising questions about whether OCIO effectively planned near-term funding needs to achieve specific goals. According to OCIO officials the cybersecurity appropriation includes no funding for personnel resources to perform analysis and oversight of cybersecurity programs, activities, and compliance. However, without sound planning procedures and internal controls, OCIO is at risk of not being able to efficiently address DOT's most serious cybersecurity gaps.

[6] The WCF, managed by the Office of the Assistant Secretary for Administration and OCIO, provides a wide range of technical and administrative services to the Department, including personnel operations and systems, IT security infrastructure, telecommunications, and procurement and acquisition services.

BACKGROUND

OMB Circular A-11[7] provides budget guidance to Federal agencies, including budgeting for IT investments and portfolio management. OMB Circular A-11 requires each agency—as part of its budgeting process—to prepare a strategic and performance plan to communicate strategic objectives and performance goals with all budget request elements. According to the Circular, planning for capital assets includes preparation of information needed to design investments; assess the benefits, risks, and risk adjusted life-cycle costs of alternative solutions; and establish realistic cost, schedule, and performance goals for the selected alternative.

FISMA and other statutes and regulations require agencies to integrate IT security in their capital planning and investment control processes. Guidance developed by the National Institute of Standards and Technology[8] (NIST) also states that due to increased competition for limited Federal resources, agencies must apply available funding to their highest priority IT security investments while maintaining appropriate security controls.

The Government Accountability Office's (GAO) Cost Estimating and Assessment Guide[9] state that cost estimates are necessary to support one program over another, to develop annual budget request, and to evaluate resource requirements at key decision points. Additionally, reliable costs estimates are necessary for OMB's capital programming process, and without reliable estimates, agencies risk cost overruns, missed deadlines, and performance shortfalls.

During fiscal year 2011, DOT requested $30 million in cybersecurity appropriations for the first time, but instead received a full-year continuing resolution that did not address Departmental cybersecurity needs. In subsequent fiscal years 2012 through 2015, Congress appropriated almost $29 million exclusively to OCIO to support its cybersecurity initiatives. In particular, cybersecurity funds were provided for necessary expenses, including upgrades to the wide area network (WAN) and other information technology infrastructure; improvements to network perimeter controls and user identity authentication management, testing and assessment of information technology against business, security, and other requirements.

The WCF receives funding by charging its customers a price and receiving advances for products and services rendered, primarily through the use of

[7] OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, June 2015.
[8] NIST Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process,* January 2005.
[9] GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs* (GAO-09-3SP), March 2009.

Inter/Intra Agency Agreements (IAA). While OCIO contracts directly with vendors, it also uses the WCF to accomplish specific cybersecurity initiatives. The OCIO Financial Management Group (FMG) is responsible for preparing cybersecurity related monthly billings in accordance with the Financial Management Procedures Manual, and forwarding the submissions to the WCF Office of Financial Management (OFM) for processing.

OCIO EXPENDED FUNDS FOR CYBERSECURITY INITIATIVES AS APPROPRIATED BUT HAD BILLING ISSUES

We did not find instances where OCIO expended the $29 million in appropriated funds that were received between 2012 and 2015 for non-cybersecurity purposes. However, the OCIO FMG did not always bill consistently under applicable IAAs in its fund disbursements through the WCF.

OCIO Expended Specifically Appropriated Funds on Cybersecurity Initiatives

OCIO expended funds on various cybersecurity initiatives, including: improvements to trusted internet connections;[10] desktop security; the on-going development of DOT's compliance monitoring capabilities;[11] and the applicable products and services OCIO acquired for these initiatives. To determine the expended funds, we analyzed the OCIO Financial Tracking Detailed Spreadsheet, which OCIO used to track expenditures specific to the $29 million in appropriated cybersecurity funds (see exhibit C). Using Delphi, DOT's accounting system, we identified 181 transactions that support the $23.4 million in expenditures pertaining to the $29 million.[12] Using statistical sampling,[13] we selected 61 transactions totaling $18.26 million.[14]

We reviewed supporting documentation for the 61 transactions, including applicable contracts, inter and intra-agency agreements, vendor invoices, and other project-related documents. We found no transactions that indicated that the funds were used for non-cybersecurity purposes.

[10] Trusted internet connections—required by OMB M-08-05 (2007)—optimize and standardize the security of agencies' individual external network connections, including connections to the internet, improve incident response capability, and provide enhanced monitoring and situational awareness of external network connections.

[11] Compliance monitoring detects system weaknesses and possible security breaches with automated tools so they can be resolved quickly.

[12] At the time of our review, the full $29 million had not been expended.

[13] Exhibit A includes a description of our sampling methodology.

[14] Of the $18.26 million, approximately $130,000 advanced to the working capital fund had not been expended.

OCIO Did Not Always Bill Consistently Under Intra-Agency Agreements when Expending Cybersecurity Funds Through the Working Capital Fund

OCIO did not always bill consistently when expending cybersecurity funds advanced through the WCF. We verified that $3.73 million in cybersecurity funds expended through the WCF supported cybersecurity initiatives. However, we found that $285,352 or 7.65 percent of the funds were inconsistently billed outside the periods of performance[15] and for services not included in the scope of work,[16] as stated in the IAAs (see table 1).

Table 1. Inconsistent Billing Amounts Under OCIO Intra-Agency Agreements

IAA year	Total billing amounts	Amount outside scope of work	Amount outside period of performance	Total amount inconsistently applied	Percentage inconsistently applied
2012	$158,525	$72,848	$0	$72,848	45.95%
2013	$405,765	$107,825	$0	$107,825	26.57%
2014	$1,836,540	$7,901	$79,063	$86,964	4.74%
2015	$1,328,526	$0	$17,716	$17,716	1.33%
Total	**$3,729,356**	**$188,574**	**$96,779**	**$285,352**	**7.65%**

Source: OIG analysis of OCIO data.

Specifically, we found that:

- The fiscal year 2012 IAA was billed $72,848 for internet circuit upgrades that were outside the IAA’s scope of work. The IAA for these services was established to fund the difference between the costs to operate the circuits, before and after the upgrades. However, between March and September 2013, cybersecurity funds were used to fund the entire cost of circuit operations.

- The fiscal year 2013 IAA was billed $107,825 for services outside the scope of work. We found that $107,758 of this amount was used to pay for the entire costs of circuit operations for the same upgraded circuit funded by the 2012 IAA. However, the fiscal year 2013 IAA was not intended to fund any portion of this circuit operation or upgrade. Another $66 of the 2013 IAA was billed for server support charges for virtual desktop infrastructure (VDI) services not described in the scope of work in that year’s IAA.

[15] Period of performance is the dates of service allowed by the contract with the vendor, usually 1 fiscal year, and identifies which work orders are funded by the IAA.

[16] Scope of work describes supplies, services, and deliverables required, and estimates for costs of services; and is identified in the IAA which is established based upon work orders.

- In fiscal year 2014, OCIO billed $7,901 for server support charges for VDI that were not described in the scope of work in that year's IAA.

- In fiscal years 2014 and 2015, circuit and server related charges totaling $96,779 were billed for services that occurred prior to the period of performance.

This was due to a lack of oversight on the part of OCIO's billing analysts and OCIO's billing procedures that do not adequately address billing within the applicable IAA. For example, the billing procedures do not provide a standard process identifying whether the period of performance is determined by the date services were provided, or by the date an invoice was received by DOT. Additionally, the billing procedures do not address determining whether an invoice falls within an IAA's specified scope of work. OCIO billing analysts, members of OCIO's FMG, are responsible for obtaining invoices from contracted vendors, calculating amounts to be billed to customers, and providing billing data to OFM to be billed and processed against the appropriate IAA. However, the OCIO billing procedures do not address how the billing analyst should determine which IAA should fund each invoice.

A lack of clear guidance on how to determine which IAA should be billed for each invoice resulted in these errors. These errors make it difficult for OCIO to ensure that WCF customers are accurately and consistently charged for services as described in customer agreements and/or IAAs.

OCIO DID NOT ADEQUATELY PLAN FOR CYBERSECURITY FUNDING

OCIO did not adequately document or plan for its cybersecurity funding needs. In particular, OCIO did not maintain adequate documentation to support its estimates for its cybersecurity budget requests. In addition, OCIO did not always follow OMB's or its own guidance when planning for its IT investments, and did not adequately plan for its near-term cybersecurity funding needs.

OCIO Did Not Maintain Adequate Documentation for Its 2014 and 2015 Cybersecurity Budget Request Estimates

While OCIO provided adequate documentation to justify its cost estimates for its 2013 cybersecurity budget request, documentation provided for 2014 and 2015 was not adequate. OMB requires agencies to maintain documentation supporting its budgeting processes, including required annual submissions to OMB—entitled Exhibit 53A—and make the documentation available upon request. Furthermore, according to GAO, a reasonable and supportable budget facilitates a program's efficient and timely execution.

An OCIO official informed us that to support its budget estimates, OCIO uses historical information such as government-wide acquisition contracts and prior cost data from similar projects. When we requested OCIO officials to provide us with their internal control procedures documenting its process for developing budgeting estimates, we were informed they used the Department's budget guidance. However, while OCIO uses the Department's budget guidance, this guidance does not provide the level of detail that OCIO officials described to OIG regarding the formulation of OCIO's budget estimates. When we requested support documentation for its budget estimates, an OCIO official informed us that the Department does not require OCIO to maintain this support documentation. Eventually, OCIO officials provided multiple spreadsheets with details breaking down how its estimates were formulated to support its $9.75 million original budget request for fiscal year 2013.

OCIO officials did not provide us adequate documentation to support its 2014 and 2015 budget estimates. To support its budget estimates for 2014 and 2015, OCIO provided two high level summary tables that are used primarily to support the Department's President's Budget Submission. For example, one table entitled "Projected Contract Services for FY 2014" summarized the amount OCIO requested for contractual services and supplies, and the acquisition of assets for DOT's WAN components. The costs were reported as WAN maintenance totaling $1.85 million, and WAN hardware, software, implementation and staffing costs totaling $7.05 million. The other table entitled "Summary of Requested Funding Changes from Base-Exhibit II-6" highlighted changes in appropriated amounts between the prior and current year.

OCIO Did Not Consistently Maintain Required OMB Planning Documentation—Exhibit 53As—for Its Cybersecurity Budget Requests

OCIO officials also did not provide us with documentation that demonstrated that they submitted a complete Exhibit 53A—as required by OMB—to support their 2013 budget request. OMB requires agencies to submit the Exhibit 53A to ensure full and accurate accounting of its IT investments. The Exhibit 53A that OCIO submitted for fiscal year 2013 did not include the $6 million in cybersecurity funding it requested or the $10 million it received for fiscal year 2012. OCIO did provide evidence that it submitted Exhibits 53As that supported its fiscal years 2014 and 2015 budget requests.

According to an OCIO official, OCIO's budget formulation process and documentation could be improved to address OMB requirements. It is important that the OCIO adhere to OMB requirements because insufficient supporting documentation and non-compliance with OMB Exhibit 53A requirements could inhibit OCIO's ability to justify its budgets to the Secretary and OMB.

OCIO Did Not Always Follow OMB's or Its Own Planning Guidance for Certain IT Investments

OCIO officials could not demonstrate they always followed OMB's Circular A-11 or its own planning guidance for its IT investment planning and execution of three projects—cloud services, VDI, and Big Fix.[17] These three projects accounted for about $20 million (68 percent) of the $29 million appropriated cybersecurity funds. According to OMB, proper planning helps agencies assess benefits, costs, and risks and establish realistic baseline cost, schedule, and performance goals. Although an OCIO official informed us that he was aware of these planning requirements for IT projects, the official did not provide sufficient evidence that the Agency developed and documented the majority of the following planning documents called for by OMB to manage and support IT projects' performance goals:

- **Alternative analysis.** Compares operational effectiveness, suitability, and life cycle cost estimates of alternatives; identifies most suitable acquisition option to satisfy needs; and is typically used to justify initiating an acquisition program.

- **Risk assessment**. Continuous risk identification, assessment, planning, monitoring, and response.

- **Program baselines**. Development of realistic baseline cost, schedule and performance goals as the standards against which actual work is measured and the bases for annual reports to OMB.

- **Benefit-cost analysis**. Evaluations of whether the benefits of completing a project are worth cost, schedule delays, and performance reduction that could be incurred.

- **Independent cost estimates**. Developed to support new or modernization programs' lifecycle cost estimates which provide all costs elements to develop, produce, deploy, and sustain the program. An estimate can cover a program's entire life-cycle or one program phase.

- **Independent Government cost estimates.** A Government prepared estimate used to check the reasonableness of contractors' cost proposals and ensure that offered prices are within a program's budget ranges.

[17] Big Fix is a continuous monitoring capability DOT is implementing on its department-wide network.

- **Earned value management**. A project management tool that compares budgeted costs to actual costs, provides objective reports on projects' status, produces warning signs of schedule delays and cost overruns, and provides unbiased estimates of a program's total costs.

DOT included similar requirements in its Enterprise Program Management Review (EPMR) Framework,[18] which applies to all DOT IT investments. The EPMR provides a standard approach for planning, managing, and governing each IT investment over its entire life cycle. For example, the Framework states IT investments must be structured to follow clearly established requirements to meet cost, schedule, and performance baselines, and be responsive to variances from established baselines to reduce the risk of cost overruns, schedule delays, and scope creep. However, because we did not receive adequate supporting documentation, we conclude that OCIO did not follow its program planning guidance for the following three projects:

- **Cloud services.** OCIO invested about $2 million in cybersecurity funds in the acquisition of cloud services over several years through September 2014, but terminated the acquisition because the services were not cost effective. We could not determine whether the costs were reasonable because OCIO officials could not provide evidence that they conducted benefit-cost analyses, alternative analysis or risk analyses to identify variances and possible savings to make decisions to terminate.

- **VDI**. OCIO invested $6.8 million and committed $7.5 million to buy licenses for VDI remote access for up to 2000 users within DOT Headquarters. OCIO conducted a pilot test on two products to test and evaluate the feasibility of using VDI as a telecommuting resource, and selected one of the products for its VDI solution. Prior to the investment, test pilot participants raised concerns about the lack of cost information to support a full-scale deployment. Still, OCIO used the initial cost estimate of $4 million that came from this test pilot for its investment planning. The Agency's $6.8 million investment was an increase of about 63 percent from its original $4 million estimate. OCIO officials acknowledged that VDI task estimates were initially incomplete and did not fully encompass the range of tasks and money involved in the project. OCIO officials also attribute the cost growth to capability and operational support gaps that needed to be addressed.

  Furthermore, OCIO did not mitigate the risks associated with the technology's ability to allow 2,000 users to remotely access DOT networks and systems without using personal identity verification (PIV) cards, which provide

[18] The EMPR Framework was introduced in June 2016. It superseded DOT's Integrated Program Planning and Management Practitioners Guide.

multifactor identity authentication.[19] DOT's cybersecurity policy[20] states that the Department must implement multifactor identity authentication for remote access to departmental networks and systems but the implementation has not been completed. OCIO has identified this security weakness and developed a corrective action plan. According to OCIO officials, DOT is in the process of assessing and planning for the transition to mandatory PIV login for VDI.

- **Continuous Monitoring Software.** OCIO acquired continuous monitoring software to address longstanding recommendations in OIG's annual FISMA reviews to enhance the Agency's information security continuous monitoring program. According to OCIO data, this software will cost just over $10 million through June 2017. While OCIO's strategy for acquiring this continuous monitoring software included a 60-day evaluation to demonstrate and test its proof of concept for 1,000 client devices, and use of its contractor's pricing data to develop the initial costs estimates, we could not assess the reasonableness of the current costs. OCIO did not perform an alternative analysis to compare other vendors' costs, or develop baseline cost estimates for the program to compare original costs to actual costs, or develop independent cost estimates to determine the lifecycle cost of the program. OCIO acknowledged several constraints with its pricing models, and noted that to obtain the most accurate pricing, asset quantities must be ascertained at the granular level, including number of workstation assets compared to number of servers.

  OCIO officials acknowledged the importance of the continuous monitoring software to the Department's mission because it is now part of its Continuous Diagnostic and Mitigation (CDM) program.[21] OCIO will jointly fund this program with the Department of Homeland Security—the Federal Government's lead on CDM. Therefore, it is important for OCIO to apply OMB planning requirements to its CDM program because clarity of the lifecycle costs will be critical for accurate and complete reporting of information to OMB. These requirements include completion of the OMB required documentation to justify a major IT investment, and a business case analysis[22] with accompanying acquisition, program management, and risk

[19] A PIV card, part of multifactor user identification, contains data to securely identify the cardholder before access to Federal facilities and information systems to assure safeguarding of Federal resources.

[20] DOT's Departmental Cybersecurity Compendium Workbook, Supplement to DOT Order 1351.37, Departmental Cybersecurity Policy.

[21] Congress established the CDM program to provide federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

[22] A business case analysis presents facts and supporting details among competing alternatives, considers life cycle costs and quantifiable and non-quantifiable benefits, and should be rigorous enough that an independent auditor can review it and understand why a particular alternative was chosen.

management plans, and other documentation that justify the investment cost, schedule, and performance goals.

According to OCIO officials, OCIO faced a number of challenges in meeting OMB requirements to develop planning documents, including the following:

- Lack of staff to meet OMB requirements to develop planning documents and perform analyses.

- Lack of funding for Federal full-time equivalent employees; many of the recommendations in our FISMA reviews require personnel resources to perform analysis and oversight.

OCIO acknowledged that it does not meet a number of OMB requirements for tracking investments. For example, OCIO does not track variances between the initial costs and current costs of its IT projects, they only track the budgeted amounts committed or paid to support its IT projects. As a result OCIO cannot effectively track significant variances with its IT projects, and report them to OMB as required or to DOT stakeholders. OCIO officials also stated the nature of the work defies predictable lifecycle costs to deal with the dynamic priorities. However, OCIO’s conclusion further highlights the Agency’s need to effectively plan its IT investments to ensure funds are efficiently spent. Additionally, they believe that OMB guidance does not successfully address this. However, during our review, an OCIO official agreed that not addressing OMB requirements could put the Department at risk of not obtaining OMB support for long-term improvements to its IT operations and Cybersecurity programs.

The lack of planning activities consistent with OMB requirements for these three projects makes it difficult for OCIO to be certain it has useful costs estimates, is managing the projects wisely, and is providing complete information on its IT investments to Congress and DOT decision makers.

OCIO Had Strategic Plans but Did Not Adequately Plan for Near-Term Cybersecurity Funding Needs

OCIO did not complete a plan for near-term cybersecurity funding goals. OCIO officials provided us OCIO’s Cybersecurity Strategic Plan for fiscal years 2011 through 2013, and Information Resources Management Strategic Plan. These plans identified the Agency’s long-term strategy that focuses on trusted internet connections, continuous monitoring, conversion to the use of PIV cards, and concepts for achieving an effective cybersecurity program. However, OCIO officials acknowledged in its Strategic Plan that to support important tactical cybersecurity goals and remediation challenges, that they are developing and implementing a separate set of plans to focus on near term threats. However, the officials did not provide us copies of these plans for near-term goals. Without these plans, we did not have needed visibility into OCIO's current-year IT goals, priorities, performance targets, and milestones. OCIO's lack of plans to prioritize and focus its near-term cybersecurity goals inhibits the Department's ability to meet OMB's requirements for Annual Performance Plans.

OCIO also does not have a written process in place for planning the prioritization of its IT investments based on near-term needs. OCIO officials stated that they prioritize IT investments to address our FISMA recommendations, departmental needs, and Federal cybersecurity initiatives and mandates, but they acknowledged that they have not formally documented the process. The absence of a clear prioritization process impedes OCIO's ability to ensure that it uses Federal funding to address DOT's most pressing cybersecurity needs.

CONCLUSION

Federal agencies are responsible for safeguarding their IT systems and sensitive information from compromise. They are also responsible for good stewardship of the limited available funding for cybersecurity. Effective financial planning and adherence to Federal budgeting requirements can significantly reduce the possibility of unnecessary cost growth and inefficient spending that could result in less secure and more vulnerable IT systems. Until it improves compliance with Federal budgeting requirements and planning practices, OCIO may inhibit DOT's ability to effectively use limited funds to mitigate IT vulnerabilities.

RECOMMENDATIONS

We recommend DOT's Chief Information Officer:

1. Update OCIO-WCF billing procedures to ensure billings are accurately and consistently applied to intra-agency agreements for products and services, within specified scopes of work and periods of performance.

2. Document OCIO's process for preparing cost estimates that support its cybersecurity budget request and maintaining support documentation justifying the basis of estimates.

3. Implement the DOT Enterprise Program Management Review Framework and procedures for maintaining support documentation that complies with OMB design and planning requirements to justify its IT investments, including the Virtual Desktop Infrastructure and the Continuous Monitoring Software, and require the use of planning tools such as cost-benefit analyses to monitor the costs, schedule, and performance goals.

4. Develop and manage a business case consistent with OMB guidance for cybersecurity investments, and ensure that Continuous Diagnostic and Mitigation program is incorporated into that investment for reporting of costs, and other criteria as required by OMB.

5. Develop and implement a process specifying how OCIO prioritizes its cybersecurity IT investments, and follow through on its plan to develop separate plans that include which cybersecurity projects it plans to focus on to address near-term threats, important tactical cybersecurity goals, and remediation challenges.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided OCIO with our draft report on May 8, 2017, and received its response on June 22, 2017, which is included as an appendix to this report. In its response, OCIO concurred with recommendation 1 as written. Accordingly, we consider recommendation 1 resolved but open pending completion of the planned actions.

OCIO concurred with recommendation 2. However, OCIO commented that OMB budget and capital planning guidance does not require the inclusion of detailed cost estimates with agency submissions, and the documents are not required for the agency capital planning and development process. OIG is not recommending that OCIO include detailed cost estimates with its submissions. Our concern stemmed primarily from the Agency's inability to support its 2014 and 2015 estimates. OCIO further states that it provided substantive documentation in support of its budget and capital planning activities, and cost estimates for obligation of appropriated funds. However, these estimates, in particular for 2014 and 2015, were not adequate. Nevertheless, the Department's planned action meets the intent of our recommendation. Accordingly, we consider recommendation 2 resolved but open pending completion of the planned action.

OCIO non-concurred with recommendations 3 and 4. OCIO stated that the cybersecurity appropriation did not meet the threshold established by OMB to be identified as a standalone, major investment. We disagree. OMB Circular A-11, Part 7, states that major acquisitions are capital assets that require special management attention because of their importance to agency mission; high development, operating, or maintenance costs; high risk; high return; or their significant roles in the administration of agency programs, finances, property, or other resources. Given the importance and significance of cybersecurity appropriations to the Department's mission, OCIO needs to immediately implement more effective IT investment planning and management controls as stated in recommendation 3 to avoid any appearance of the waste or mismanagement of cybersecurity appropriated funds.

OCIO also stated that it plans to implement the updated OMB direction and guidance for IT and cybersecurity spending, encapsulated in the revisions to OMB Circular A-11 and corresponding OMB implementation guidance, by September 30, 2021. However, based on additional information we received on the Department's interactions with OMB on this matter, the guidance has not been finalized and OMB has not instructed DOT to implement this unapproved guidance. Furthermore, OCIO does not explain why it cannot use its own guidance, the Enterprise Program Management Review Framework, to justify its IT investments until OMB issues new guidance. Given the importance of transparency and accountability of these key cybersecurity investments, we consider recommendations 3 and 4 open and unresolved and request that the agency reconsider its position.

OCIO concurred with recommendation 5, but commented that OMB does not cite specific requirements on the prioritization of cybersecurity investments via OMB Circulars A-11 and A-130. OCIO attributes its approach to this absence of criteria. OCIO is not correct. OMB mandated the use of NIST guidance. NIST Special Publication 800-65, Integrating IT Security into the Capital Planning and Investment Control Process, provides guidance on prioritizing IT expenditures. Other NIST publications assist agencies by describing how to assess risk and prioritize the implementation of security controls, and in turn, help prioritize investments. These publications provided more than sufficient information to develop a suitable process to prioritize DOT's cybersecurity investments. OCIO further notes that OMB has issued updates to OMB Circular A-11, and the Administration issued a Cybersecurity Executive Order that requires agencies to adopt the NIST Cybersecurity Framework and leverage the framework to prioritize cybersecurity spending. OCIO indicated that it plans to take these actions by December 31, 2019. While we agree with the planned actions, the implementation timeframe is excessive. Given the importance of prioritizing limited cybersecurity resources, we consider this recommendation open and unresolved and request that the Agency reconsider its target action date.

ACTIONS REQUIRED

We consider recommendations 1 and 2 resolved but open pending completion of planned actions. We consider recommendations 3, 4 and 5 open and unresolved and request that OCIO reconsiders its response and provide, within 30 days of this report, the information described above in accordance with DOT Order 8000.1C.

We appreciate the courtesies and cooperation of DOT's Office of the Chief Information Officer Representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407, or Kevin Dorsey, Program Director, at (202) 366-1518.

#

cc: The Secretary
DOT Audit Liaison, M-1

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted our work from November 2015 through May 2017 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 objectives were to determine whether OCIO (1) expended the appropriated funds to support cybersecurity initiatives, and (2) adequately planned for its cybersecurity funding needs.

To conduct our work, we interviewed representatives from DOT's Office of the Chief Information Officer; OST's Resource Management Office, Office of Budget, Office of the Chief Financial Officer, Information Technology Shared Services, Office of Financial Management (Working Capital Fund), and Acquisition Services; operating administration CIO representatives; and FAA's Enterprise Services Center representatives, who maintain Delphi, DOT's Accounting system.

To determine whether OCIO expended appropriated funds to support cybersecurity initiatives, we tested a sample of transactions OCIO determined to pertain to cybersecurity related products and services. To select this sample, we took the following steps:

- Using Delphi, the Department's accounting system, we identified 181 cybersecurity related transactions with an absolute value of $29.45 million which included expenditures, credits, voids, and de-obligated amounts.

- After excluding the credits, voids, and de-obligated amounts we were left with $23.36 million in actual expenditures.

- We selected a sample of 61 from the universe of 181 transactions that had a total absolute value of $23.62 million of which $18.26 million were expenditures so that our sample covered 78.16 percent of the $23.36 million expenditures in our universe.

- For all sampled Delphi transactions, we reviewed supporting documentation such as applicable contracts, inter and intra-agency agreements, vendor invoices, and other project-related documents.

To determine whether OCIO adequately planned for its cybersecurity funding needs, we reviewed Federal and DOT budget guidance including OMB A-11, Preparation, Submission, and Execution of the Budget. We analyzed OCIO's budget request submissions for fiscal years 2013 through 2015 and investment planning and prioritization documentation for products/services procured using the cybersecurity appropriation. We assessed OCIO's planning policies and procedures for compliance with OMB, GAO, and DOT guidance. We reviewed internal and external audits and reviews, as well as additional documentation OCIO representatives identified as applicable to the budget planning and/or execution process.

We evaluated OCIO's plans for obligating and expending cybersecurity appropriations for fiscal years 2012 through 2015, including a review and analysis of OCIO's Cybersecurity Financial Tracking Detailed Spreadsheet, which is their primary tool to track cybersecurity procurements, and expenditures, and evaluated the accuracy of information contained on the Financial Tracker to Delphi data to identify potential areas of concern.

EXHIBIT B. ENTITIES VISITED OR CONTACTED

DOT Headquarters, Washington, DC:

- Office of the Chief Information Officer (OCIO),
- OA Chief Information Officers and IT Managers,
- OCIO Working Capital Fund Management including Billing Analysts and Project Managers,
- WCF Office of Financial Management,
- OST Office of Budget, and
- OST Office of Acquisition Services.

FAA’s Enterprise Services Center, located at the Mike Monroney Aeronautical Center, Oklahoma City, OK. OIG met with officials responsible for accounts payable to external vendors and other Federal agencies.

EXHIBIT C. PRODUCTS AND SERVICES THAT OCIO IDENTIFIED[a] AND ACQUIRED WITH CYBERSECURITY FUNDS

	Original cost committed	Adjusted cost committed	Awarded in Delphi	Expended[b]
TIC				
Internet/TIC Circuits	$3,302,500.00	$5,346,263.92	$4,116,387.92	$3,966,120.49
Terremark/Cloud Provider	730,500.00	1,998.737.24	1,998,737.24	1,998,737.24
Other	5,750,000.00	582,536.88	582,536.88	571,336.82
Total TIC	9,783,000.00	7,927,538.04	6,697,662.04	6,536,194.55
Desktop Security				
Virtual Desktop Infrastructure (VDI)	4,149,178.00	7,509,308.99	6,779,905.94	6,768,997.24
Internet (TIC Circuits)	610,000.00	652,042.31	420,995.00	420,995.00
Other	1,194,000.00	1,348,884.09	1,320,884.48	1,301,638.24
Total Desktop Security	5,953,178.00	9,510,235.39	8,521,785.42	8,491,630.48
Compliance Monitoring				
Manager Security Suite (Big Fix)	4,984,467.00	10,171,662.06	8,035,221.45	7,961,629.45
Continuous Diagnostic & Mitigation (CDM)	150,000.00	992,024.93	992,024.93	856,646.95
Other	0.00	253,948.16	253,948.16	243,080.86
Total Compliance Monitoring	5,134,467.00	11,417,635.15	9,281,194.54	9,061,357.26
Total Products and Services	20,870,645.00	28,855,408.58	24,500,642.00	24,089,182.29

[a] The products and services acquired in support of the initiatives OCIO determined to be cybersecurity were categorized into the following focus areas: (1) trusted internet connection (TIC); (2) desktop security; and (3) compliance monitoring.

[b] Expended amounts reflect all cybersecurity funds expended as of January 6, 2016.

Source: OIG generated based on data from OCIO's financial tracking detailed spreadsheet.

Exhibit C. Products and Services that OCIO Identified and Acquired With Cybersecurity Funds

EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Kevin Dorsey	Program Director
Brian Frist	Project Manager
Allison La Vay	Senior Analyst
Christina Burgess	Analyst
Scott Williams	Analyst
Petra Swartzlander	Senior Statistician
Andrea Nossaman	Senior Writer-Editor
Susan Neill	Writer-Editor
Amy Berks	Senior Counsel
Seth Kaufman	Senior Counsel

APPENDIX. AGENCY COMMENTS

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

Subject: **<u>INFORMATION</u>:** Management Response – Office of Inspector General (OIG) Report on Cybersecurity Spending

Date: June 22, 2017

From: Kristen Baldwin
Acting DOT Chief Information Officer

KRISTEN K. BALDWIN
Digitally signed by KRISTEN K. BALDWIN
DN: c=US, o=U.S. Government, ou=DOT Headquarters, ou=OSTHQ, cn=KRISTEN K. BALDWIN
Date: 2017.06.22 12:46:17 -04'00'

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

The U.S. Department of Transportation (DOT) Office of the Chief Information Officer (OCIO) considers cybersecurity among its highest priorities. The OCIO works closely with the Department's Office of the Chief Financial Officer, the Office of Management and Budget (OMB), and the Department of Homeland Security to ensure that DOT investments in cybersecurity are well justified, adequately resourced, effectively managed, and achieve planned outcomes. It is the assessment of the OCIO that the Inspector General's report does not accurately represent the degree of planning and execution associated with the Cybersecurity appropriation, or the conscientious effort and coordination OCIO exercised to ensure proper application of the referenced cybersecurity funds to the benefit of the Department. For example, OCIO utilizes a spend plan format that is created at the budget formulation stage. The spend plan document is constantly updated in the year of execution to reflect actual expenditures, Administration priorities, and emerging threats. OCIO's cybersecurity investments have been instrumental for the Department in implementing new cybersecurity capabilities, reducing cyber risks, and progressing toward meeting federal cybersecurity targets. Recent examples of DOT's efforts in these areas include the following:

- Transition to Managed Trusted Internet Protocol Services (MTIPS) to improve Internet security, and reduce the Department's exposure to external threats;
- Integration of Continuous Diagnostics and Mitigation (CDM) capabilities into the DOT Common Operating Environment

(COE) to detect, assess, and report upon unmanaged or potentially insecure endpoints;

- Replacement of an end-of-life vulnerability management solution with a new DOT enterprise solution to assess endpoints for vulnerabilities and identify those for prioritized mitigation.

It is important to note that the OIG found that the OCIO expended $29 million, as appropriated, to support cybersecurity initiatives. The cybersecurity initiatives included improvements to trusted internet connections, desktop security, ongoing development of DOT's compliance monitoring capabilities and applicable products and services acquired for these initiatives. Further OIG did not find any instances of fraud, waste, abuse, or mismanagement in this audit.

Based upon our review of the draft report, we concur with recommendation 1 as written. We plan to implement the recommendation by September 30, 2018.

We concur with recommendation 2, with comment. OMB budget and capital planning guidance— inclusive of OMB Circular A-11, OMB Circular A-130, and annually issued capital planning and budget guidance— do not require the inclusion of detailed cost estimates with agency submissions, and DOT capital planning and budget policy and guidance also do not require the inclusion of these documents as part of agency capital planning and budget development processes. OCIO provided substantive documentation in support of its budget and capital planning activities, and cost estimates for obligation of appropriated funds, which are required to be retained as part of the contract record. Also, OIG did not cite any findings of non-compliance or misappropriation of funds. We will develop an internal standard operating procedure to address the recommendation by September 30, 2018.

We non-concur with recommendations 3 and 4. In accordance with OMB Circulars A-11 and A-130, the cybersecurity appropriation, as a capital investment fund supporting capability development and weakness remediation within other, existing DOT investments, did not meet threshold requirements for cost and criticality established by OMB to be identified as a standalone, major investment. Subsequently, OMB has issued updates to OMB Circular A-130 and A-11, and developed a new methodology for the reporting and management of agency IT commodity, infrastructure, and cybersecurity spending, aligned to IT "cost towers" and a new IT Security and Compliance investment construct, which does not have the same management requirements as standard investments. We plan to implement the updated OMB direction and guidance for IT and cybersecurity spending, encapsulated in the revisions to OMB Circular A-11 and corresponding OMB implementation guidance, by September 30, 2021.

We concur with recommendation 5, with comment. OMB does not cite specific requirements or guidance on the prioritization of cybersecurity investments via Circulars A-130 and A-11. In the absence of specific criteria, OCIO provided documentation to the OIG of the approach we follow to prioritize spending within the cybersecurity appropriation. Subsequently, OMB has issued updates to OMB Circular A-11, and the Administration has issued a Cybersecurity Executive Order (EO), which requires agencies to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and leverage the framework in to prioritize cybersecurity spending. We plan to implement the requirements of the revisions to OMB A-11 and the Cybersecurity EO by December 31, 2019.

We appreciate the opportunity to respond to the OIG draft report. Please contact Andrew Orndorff, Associate CIO / Chief Information Security Officer (CISO), at (202) 366-7111, if you have any questions.