U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

QUALITY CONTROL REVIEW FOR THE ASSESSMENT OF DOT'S PROTECTION OF PRIVACY INFORMATION

Report No. QC2018016

January 17, 2018

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

Quality Control Review for the Assessment of DOT's Protection of Privacy Information

Mandated by the Fiscal Year 2005 Consolidated Appropriations Act for Transportation, Treasury, Independent Agencies, and General Government

Departmentwide | QC2018016 | January 17, 2018

What We Looked At

This report summarizes the results of an audit of the Department of Transportation's (DOT) protection of privacy information. DOT has determined that 168 of its 464 computer systems contain personally identifiable information (PII) about the public and/or DOT employees. The Fiscal Year 2005 Consolidated Appropriations Act for Transportation, Treasury, Independent Agencies, and General Government, as amended, requires agencies to enhance the protection of PII they collect and use. The act also requires inspectors general to periodically audit their agencies' privacy programs or hire independent, third party organizations to conduct the reviews.

We contracted with KPMG LLP, an independent public accounting firm, to conduct this audit subject to our oversight. The audit objectives were to determine whether (1) DOT has established adequate procedures for the collection, use, and security of PII; (2) DOT ensures compliance with its own privacy and data protection policies and applicable laws and regulations to prevent unauthorized access to or unintended use of PII; and (3) DOT's Operating Administrations properly evaluate the necessity of using PII to process system data.

What We Found

We performed this QCR of KPMG's report and related documentation. Our QCR disclosed no instances in which KPMG did not comply, in all material respects, with generally accepted Government auditing standards.

Recommendations

DOT concurs with KPMG's 12 recommendations.

Contents

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: January 17, 2018

Subject: INFORMATION: Quality Control Review for the Assessment of DOT's Protection of Privacy Information | Report No. QC2018016

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

To: Federal Aviation Administrator
Chief Information Officer, DOT

This report summarizes the results of an audit of the Department of Transportation's (DOT) protection of privacy information. DOT has determined that 168 of its 464 computer systems contain personally identifiable information (PII) about the public and/or DOT employees. The Office of Inspector General (OIG) has previously conducted privacy-related audits and reviewed systems that contain PII.[1]

The Fiscal Year 2005 Consolidated Appropriations Act for Transportation, Treasury, Independent Agencies, and General Government[2] requires agencies to enhance the protection of the PII that they collect and use. The act also requires inspectors general to periodically audit their agencies' privacy programs or hire independent, third party organizations to conduct the reviews.

We contracted with KPMG LLP, an independent public accounting firm, to conduct this review subject to our oversight. The audit objectives were to determine whether (1) DOT has established adequate procedures for the collection, use, and security of PII; (2) DOT ensures compliance with its own privacy and data protection policies and applicable laws and regulations to

[1] *Quality Control Review for the Audit of DOT Protection of Privacy Information* (OIG Report No. QC-2014-053), June 5, 2014; *FISMA 2013: DOT Has Made Progress, but Its Systems Remain Vulnerable to Significant Security Threats* (OIG Report No. FI-2014-006),November 22, 2013; *FAA's Civil Aviation Registry Lacks Information Needed for Aviation Safety and Security Measures* (OIG Report No. FI-2013-101), June 27, 2013; *Information Security and Privacy Controls Over the Airmen Medical Support Systems* (OIG Report No. FI-2010-060).

[2] Public Law 108-447. Div. H, Title V, § 522 (2004), as amended by Public Law No. 110-161, Div. D, Title VII, § 742(b) (2007).

prevent unauthorized access to or unintended use of PII; and (3) DOT's Operating Administrations properly evaluate the necessity of using PII to process system data.

KPMG found that DOT did not consistently implement and enforce its PII policies and procedures across its Operating Administrations. KPMG made the following recommendations to improve DOT's Privacy Program.

KPMG recommends that Federal Aviation Administration:

FAA Privacy Program

1. Conduct a review of its privacy program to identify changes needed to ensure that systems' privacy plans are completed in accordance with the DOT Privacy Risk Management Policy.

System Owner - System #2

2. Ensure the system Privacy Plan includes all requirements established by the DOT Chief Privacy Officer in the privacy threshold assessment (PTA) and the adjudication statement is implemented.

System Owner - System # 5

3. FAA ensures that the "encryption protections for data at rest" are implemented in accordance with the DOT Privacy Risk Management Policy.

4. FAA confirms that the session time-out functionality has been implemented.

System Owner - System # 8

5. Ensure that the encryption protections for data at rest are implemented in accordance with the DOT Privacy Risk Management Policy.

System Owner - System #9

6. Provide system specific and/or specialized role based privacy job aides as needed to personnel who maintain and/or have access to PII data.

7. Ensure the Privacy Plan including all requirements established by the DOT Chief Privacy Officer in the PTA adjudication statement is implemented.

8. Implement memoranda of understanding or similar agreements for internal sharing of PII.

9. Ensure that encryption protections for data at rest are implemented in accordance with the DOT Privacy Risk Management Policy.

10. Ensure that the plan of action and milestones for encryption protections for data at rest is actively monitored and updated as changes occur prior to the estimated closure date..

KPMG recommends that Office of the Secretary of Transportation:

Departmental Chief Privacy Officer

11. Establish a continuous monitoring program for privacy supportive security controls to ensure PII systems remain compliant with DOT Privacy Risk Management policy.

System Owner - System #15

12. Ensure that the encryption protections for data at rest and during transit have been implemented in accordance with the DOT Privacy Risk Management Policy.

We performed this quality control review (QCR) of KPMG's report, dated, September 26, 2017 (see attachment), and related documentation. Our QCR, as differentiated from an audit engagement performed in accordance with generally accepted Government auditing standards, was not intended for us to express, and we do not express, an opinion on DOT's information management practices for the protection of PII. KPMG is responsible for its independent auditor's report and the conclusions expressed in that report. Our QCR disclosed no instances in which KPMG did not comply, in all material respects, with generally accepted Government auditing standards.

We appreciate the courtesies and cooperation of Department of Transportation representatives during this audit. If you have any questions concerning this report, please call Louis C. King, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1407.

cc: The Secretary
DOT Chief Privacy Officer
DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-100

Agency Comments and OIG Response

We provided DOT with our draft report on November 14, 2017, and received its formal response on December 18, 2017. DOT's response is included in its entirety as an appendix to this report. DOT concurs with all 12 of KPMG's recommendations and provided appropriate actions and completion dates.

Additionally, DOT's management response states that all of OIG's 10 recommendations from prior years have been closed and implemented. The recommendations have been closed, but, as it states in its report, KPMG identified issues related to the PII security controls for encryption of data at rest and during transmission, and enablement of session time outs.

Actions Required

We consider all 12 of KPMG's recommendations resolved and open pending completion of planned actions.

Exhibit. List of Acronyms

DOT	Department of Transportation
FAA	Federal Aviation Administration
OIG	Office of Inspector General
PII	personally identifiable information
PTA	privacy threshold assessment
QCR	quality control review

Appendix. Agency Comments

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

Memorandum

Subject: **INFORMATION:** Management Response to the Office of Inspector General (OIG) Draft Report—Quality Control Review for the Assessment of DOT's Protection of Privacy Information

Date: December 18, 2017

From: Stephen Holden
Associate Chief Information Officer for IT Policy and Oversight

STEPHEN HUDSON HOLDEN
Digitally signed by STEPHEN HUDSON HOLDEN
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=STEPHEN HUDSON HOLDEN
Date: 2017.12.18 15:02:44 -05'00'

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

The U.S. Department of Transportation (DOT) is committed to continuing to strengthen the Department's privacy risk management program and ensure that personally identifiable information (PII) entrusted to the Department is protected appropriately.

Upon review of KPMG's report, we concur with the recommendations as written. The Federal Aviation Administration plans to implement recommendations 1 through 10 by July 21, 2018. The Office of the Secretary plans to implement recommendation 1 by June 30, 2018 and recommendation 2 by August 31, 2018.

KPMG's report cites that nine of the 10 prior year OIG recommendations were implemented and closed. This statement and the statement in recommendation 9 in Appendix 3 are inaccurate. DOT implemented recommendation 9 and the OIG closed it. We request that KPMG's report reflect this fact—all 10 recommendation were implemented and closed.

We appreciate the opportunity to review the OIG draft report. Please contact Claire W. Barrett, Departmental Chief Privacy Officer, at 202-366-8135 with any questions.

Attachment.

Independent Auditor's Report

Performance Audit Pursuant To The Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005, Section 522-d Fiscal Year 2017

The Department of Transportation (DOT) Implementation of Personally Identifiable Information (PII) Program and Practices

For the Period February 23, 2017 through September 26, 2017

Prepared for: U.S. Transportation
Office of the Inspector General

As of September 26, 2017

KPMG LLP
1676 International Drive
Mclean, VA 22102

TABLE OF CONTENTS

Mr. Louis King
Assistant Inspector General for Financial and Information Technology Audits
1200 New Jersey Avenue, SE
Washington, DC 20590

This report presents the results of our work conducted to address the performance audit objectives relative to the independent evaluation of the U.S. Department of Transportation (DOT) Implementation of Personally Identifiable Information (PII) Programs and Practices in support of the fiscal year (FY) 2017 Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005, Section 522-d. The engagement audit period was from September 28, 2016 through September 26, 2017. We performed our work from February 23, 2017 through September 26, 2017, and our results are as of September 26, 2017.

Section 522-d provides guidelines and a comprehensive approach for Executive agencies to establish and develop information management practices relating to data privacy issues. Requirements include the implementation of privacy policies and procedures for public and employee data, the designation of a senior official for privacy, preparation of a report by the DOT Privacy Office to the Office of the Inspector General (OIG), and an annual benchmark report to Congress regarding the status of the DOT privacy program. The Act also requires that each agency shall have performed an independent, third party review periodically, regarding the use of information in identifiable form and the privacy and data protection procedures of the agency.

KPMG LLP (KPMG) has been tasked by the Department of Transportation (DOT), OIG to conduct a performance audit of DOT's information management practices for protection of PII, as they relate to the guidelines set forth in the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005, Section 522-d and the Consolidated Appropriations Act of 2008, Section 522-d. The performance audit assessed DOT's oversight and the Operating Administrations (OAs) maturity in the establishment and implementation of a performance-measurement system for privacy practices. In addition, we were also tasked with reviewing the DOT implementation and execution of ten recommendations made in the OIG report *Quality Controls Review for the Audit of DOT Protection of Privacy Information Report.*

We conducted our audit work in accordance with Generally Accepted Government Auditing Standards (GAGAS), and the American Institute of Certified Public Accountants (AICPA) Standards for Consulting Services. 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 objectives were to determine whether DOT (1) has established adequate procedures for the collection, use, and security of PII; (2) ensures compliance with its own privacy and data protection policies and applicable laws and regulations to prevent unauthorized access to or unintended use of PII; and (3) OAs properly evaluate the necessity of using PII to process system data. We used National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev.) 4, including updates as of December 2014, *Security and Privacy Controls for Federal Information Systems and Organizations* and Office of Management and Budget (OMB) requirements to develop our audit criteria, which sets forth eight privacy control areas: (1) Authority & Purpose (AP) (2) Accountability, Audit, and Risk Management (AR); (3) Data Quality & Integrity (DI); (4) Data Minimization & Retention (DM); (5) Individual Participation & Redress (IP); (6) Security (SE); (7) Transparency (TR); and (8) Use Limitation (UL).

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives aforementioned above. We conclude that for the testing period February 23, 2017 through September 26, 2017, DOT has taken efforts to develop a framework for the collection, use, and security of PII data Department-wide; however DOT did not consistently implement and enforce its PII policies and procedures across its OAs in accordance with current DOT, NIST, and OMB requirements. We identified nine (9) deficiencies, and twelve (12) recommendations which are listed within the "Findings and Recommendations" section of the report. These deficiencies were identified in three (3) of the eight (8) privacy security control areas of the Department's and OAs Implementation of PII Programs and Practices pertaining to AR; DM; and IP. KPMG's methodology section provides additional information for the eight (8) NIST privacy security controls, which can be located on pages 7-8. The deficiencies identified in this report were communicated to DOT management prior to the issuance of this report.

Appendix 3, Status of Prior-Year Findings, summarizes the DOT's progress in addressing prior year recommendations from the OIG report *QC-2014-053, Quality Controls Review for the Audit of DOT Protection of Privacy Information Report.* Appendix 2 contains a glossary of terms used in the report.

This performance audit did not constitute an audit of financial statements in accordance with *GAGAS.* KPMG was not engaged to, and did not render an opinion on DOT internal controls over financial reporting or over financial management systems. KPMG cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

KPMG LLP

BACKGROUND

Section 522-d of the Fiscal Year 2005 Omnibus Spending Bill for Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005 and the Consolidated Appropriations Act of 2008. Section 522-d provides guidelines and a comprehensive approach for Executive agencies to establish and develop information management practices relating to data privacy issues. Requirements include the implementation of privacy policies and procedures for public and employee data, the designation of a senior official for privacy, preparation of a report by the DOT Privacy Office to the OIG, and an annual benchmark report to Congress regarding the status of the DOT privacy program. The Act also requires that each agency shall have performed an independent, third party review periodically, regarding the use of information in identifiable form and the privacy and data protection procedures of the agency.

The Privacy Act of 1974, 5 U.S.C. § 552a, as amended, and OMB Memorandum M-06-15 Safeguarding PII, requires agencies to collect only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President. Agencies are required to protect this information from any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained, and must not disclose this information except under certain circumstances. The information collected is considered a record under the Privacy Act if it is an item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. When an agency has a group of any records under its control from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual, the agency has a system of records. The Privacy Act requires that a public notice, commonly referred to as a System of Records Notice (SORN), be published in the Federal Register that describes the existence and character of the system of records.

With increased data collection, technology acceleration and regulatory complexity comes increased privacy risk, which is why DOT focuses on incorporating proactive privacy risk management controls, as required by NIST 800-53 rev 4 (Appendix J) into every stage of program and information privacy system development. DOT has improved compliance with privacy objectives by raising awareness among employees and leadership regarding the standards for data safety. DOT has implemented privacy risk management frameworks for training, compliance assessment, and vulnerability breaches remediation. Risk management activities take place in four stages consisting of the following:

(1) *Align DOT-wide privacy risk management guidance to the Department's Strategic Plan and Annual Performance Plan*. Each DOT OA may implement more rigorous privacy risk management standards as necessary based on specific mission requirements and information system privacy requirements.

(2) *Maintain risk management standards*. Privacy risk management standards are managed to ensure they are developed, verified, versioned, used and sustained over time with the perspectives of all stakeholders in mind. Changes include changes to artifacts (e.g. SORN, Privacy Threshold Analyses [PTA], and System Disposal Assessments [SDA], Privacy Impact Assessments [PIA]) and other privacy documentation and standards. Each DOT OAs should

maintain privacy data and artifacts that are relevant, current, and valid, as well as track and document changes in order for data and artifacts to be trusted for use in planning and decision-making.

(3) *Use risk management tools*. The artifacts, privacy risk management standards, and data from privacy risk analyses support the Department's decision-making on policies, including proposed rulemakings, information collections and operational matters like IT investments. Each DOT OA should use the privacy risk management standards documented in the policy to evaluate various policy and operational proposals under review by the Department.

(4) *Measure risk management effectiveness*. The DOT Privacy Risk Management program, as well as resultant analyses and mitigation strategies, are evaluated on a regular basis to ensure DOT programs and the processes and systems used to support them maintain current with privacy statutes, guidance and policies, accurately reflect DOT practice, and engender trust. Overall, the privacy risk management lifecycle supports DOT's mission by reducing the possibility of errors in behaviors, technologies, and other business activities that could lead to undesirable privacy outcomes, including but not limited to the loss of public support, unauthorized use or access to PII, and increased oversight.

OBJECTIVE

KPMG conducted a performance audit to determine whether DOT (1) has established adequate procedures for the collection, use, and security of PII; (2) ensures compliance with its own privacy and data protection policies and applicable laws and regulations to prevent unauthorized access to or unintended use of PII; and (3) OAs properly evaluate the necessity of using PII to process system data.

KPMG has been tasked by the DOT OIG to conduct a performance audit of DOT's information management practices for PII policies, practices, and data for the period from February 23, 2017 through September 26, 2017. To do so, KPMG performed the following:

a) A review of the agency's technology, practices and procedures with regard to the collection, use, sharing, disclosure, transfer and storage of information in identifiable form;

b) A review of the agency's stated privacy and data protection procedures with regard to the collection, use, sharing, disclosure, transfer, and security of personal information in identifiable form relating to agency employees and the public;

c) A detailed analysis of the agency internet, network and websites for privacy vulnerabilities, including noncompliance with stated practices, procedures and policies and risks for inadvertent release of information in an identifiable form from the website of the agency;

d) A review of agency compliance with section 522-d of the Omnibus Spending Bill for Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005 and the Consolidated Appropriations Act 0(2008).

We also reviewed 10 prior year recommendations related to DOT's PII Policies and Procedures to determine their current status. In summary, nine (9) out of the ten (10) prior year recommendations were implemented and closed. Appendix 3, documents our review and inspection procedures performed of the DOT implementation and execution of ten recommendations made in the OIG report *Quality Controls Review for the Audit of DOT Protection of Privacy Information Report.* Appendix 2 contains a glossary of terms used in the report.

This report recommended the Department's Chief Information Officer (CIO), DOT Chief Privacy Officer (CPO), and OA Privacy Officers, in coordination with the components, take the following actions:

DOT CIO

1. Implements and monitors a process for ensuring compliance with the Privacy Act, as amended and all other federal privacy related directives as well as DOT's established privacy and data protection policies.
2. Implements and monitors a process for ensuring information system security controls are implemented and operating according to federal requirements and DOT policy in order to assist with safeguarding the confidentiality of PII.
3. Conducts a review of the organizational structure and resources and requests necessary changes to improve program compliance and strengthen the line of accountability from the Operating Administration Privacy programs to the Departmental Privacy officer in order for the Departmental Privacy Officer to effectively administer the implementation and management of the DOT Privacy Policy and Program.
4. Ensures the inventory of systems containing PII and DOT websites is monitored and updated at least annually and implements procedures that will trigger a change to the inventory listing when systems are added, deleted, or when changes occur.
5. Updates DOT policy to reinforce OAs responsibilities to ensure they are able to illustrate the privacy controls required by federal laws and regulations, and DOT policies by providing evidence that the controls are in place and functioning effectively and responding to notification of findings to make sure that control weaknesses are addressed.

DOT CPO

6. Conducts an annual review of DOT Privacy policies and practices to ensure policies and procedures reflect current regulations, guidance and policy.
7. Implements procedures that ensure oversight of PIAs, and communicates the requirements and expectations for such assessments and other activities, including but not limited to, improved recordkeeping conducted by the OA Privacy Officers necessary for program success.

OA Privacy Officers

8. Ensure PIAs are completed, reviewed and approved by the Departmental Privacy Officer prior to the deployment of any system containing PII.
9. Ensure ongoing validation of specific privacy related security controls for their systems are in effect, including those that safeguard confidentiality; provide secure remote access, encryption of back up media; follow up of unauthorized mobile devices, and proper user account and password settings in accordance with DOT policy. In addition, implement procedures requiring OAs to report non-compliance in their systems to the DOT Chief Privacy Officer.
10. Conduct an annual review of their web sites, ensuring proper and accurate posting of their Privacy policies.

SCOPE

The performance audit procedures we selected for review are designed to evaluate the implementation of the PII practices over ten (10) OAs and sixteen (16) privacy systems, which are listed in Tables 1 and 2 below.

Table 1: Scope of PII Analysis by OAs

OA's
Federal Aviation Administration (FAA)
Office of the Secretary (OST)*[1]
Federal Highway Administration (FHWA)
Federal Motor Carrier Safety Administration (FMCSA)
National Highway Traffic Safety Administration (NHTSA)
Federal Transit Administration (FTA)
Maritime Administration (MARAD)
Federal Railroad Administration (FRA)
Pipeline and Hazardous Materials Safety Administration (PHMSA)
Office of the Inspector General (OIG)*
Saint Lawrence Seaway Development Corporation (SLSDC)

Table 2: Scope of PII Systems[2]

Privacy Systems
PII System #1
PII System #2
PII System #3
PII System #4
PII System #5
PII System #6
PII System #7
PII System #8
PII System #9
PII System #10
PII System #11
PII System #12
PII System #13
PII System #14
PII System #15
PII System #16

[11] *- OST and OIG are considered to be one OA; therefore the purpose of the report we're reporting 10 OAs.

[2] Due to privacy and sensitivity purposes, privacy system names were removed from the report.

METHODOLOGY

The audit was performed based on NIST Special Publication (SP) 800-53 Revision (Rev.) 4, including updates as of December 2014, *Security and Privacy Controls for Federal Information Systems and Organizations* and OMB requirements. The audit focused on assessing the design, implementation, and operating effectiveness of selected controls established over the DOT and OA's programs and practices that are outlined in the following table (Table 1). Additional criteria and references considered during the assessment are described in Appendix 1.

We evaluated the below eight (8) privacy control families identified in the NIST, SP 800-53, Revision 4, April 2013, including updates as of December 2014, *Security and Privacy Controls for Federal Information Systems and Organizations (Appendix J)*. A representative sample of NIST security controls were selected for evaluation. The selected controls include all the relative privacy controls assessed:

Table 1: NIST Privacy Control Families[3]
Authority and Purpose (AP): Individuals should be told how the collecting organization intends to use, maintain and share data; through the following sub-controls: AP-1 – Authority to Collect AP-2 – Purpose Specification
Accountability, Audit, and Risk Management (AR): Requires organizations and individuals to be accountable for compliance with applicable privacy practices; through the following sub-controls: AR-1– Governance and Privacy Program AR-2– Privacy Impact and Risk Assessment AR-3– Privacy Requirements for Contractors and Service Providers AR-4– Privacy Monitoring and Auditing AR-5– Privacy Awareness and Training AR-6– Privacy Reporting AR-7– Privacy Enhanced System Design and Development AR-8– Accounting of Disclosures
Data Quality and Integrity (DI): Ensure that PII is accurate, complete and timely; through the following sub-controls: DI-1 – Data Quality DI-2 – Data Integrity and Data Integrity Board
Data Minimization and Retention (DM): Collect only the minimum amount of data necessary to accomplish its business goals, and retain the data for no longer than is needed; through the following sub-controls: DM-1 – Minimization of PII DM-2 – Data Retention and Disposal DM-3 – Minimization of PII used in Testing, Training and Research
Individual Participation and Redress (IP): Individuals should be able to reasonably control how their data is used, be able to agree to such use, be able to have access to their own data and be able to have inaccuracies fixed; through the following sub-controls: IP-1 – Consent

[3] KPMG selected specific test procedures that were applicable to the computing environment; therefore, not all available test procedures within each control family were performed.

Table 1: NIST Privacy Control Families[3]
IP-2 – Individual Access IP-3 – Redress IP-4 – Complaint Management
Security (SE): Protects data and PII from unauthorized use, access or disclosure; through the following sub-controls: SE-1 – Inventory of PII SE-2 – Privacy Incident Response
Transparency (TR): Organizations should be open with individuals on how data is collected, used, shared and stored; through the following sub-controls: TR-1 – Privacy Notice TR-2 – Systems of Records Notices and Privacy Act Statements TR-3 – Dissemination of Privacy Information Program
Use Limitation (UL): Use PII only for the purposes specified by the organization's privacy policy; through the following sub-controls: UL-1 – Internal Use UL-2 – Information Sharing with Third Parties

Source: NIST SP 800-53, Rev. 4

The engagement was performed in three phases: (1) planning, (2) testing and interviewing and (3) report writing.

The planning phase was designed to help ensure that team members developed a collective understanding of the privacy and reporting practices in place for the ten OAs and the sixteen systems selected across the OAs. KPMG provided separate questionnaires to each OA and PII system project team in scope. The questionnaires were designed to provide a foundational understanding for conducting interviews and for identifying additional documentation requests and, in some cases, provide completed and final responses to inquiries.

During the testing and interviewing phases, we conducted interviews, collected and inspected artifacts, and designed and performed test procedures. Test procedures were primarily conducted at DOT headquarters and FAA facilities in Washington D.C. Testing procedures over privacy controls are based on the Federal legislation, policies and industry standards.

The report writing phase entailed writing a draft report, conducting an exit conference, providing a formal draft report to the OIG for review, and preparing and issuing the final report. In addition, the OIG's Quality Control Review (QCR) will include management's response to the report; which will be provided through the OIG.

RESULTS

Overall KPMG determined the Department has made progress in establishing a Department-wide Privacy Risk Management framework, policies, and procedures for the collection, use, and security of privacy related data.

The Department needs to continue to work with the OAs to ensure they are following and adhering to the Department's Privacy Risk Management policies, as we identified a number of OA-level PII findings identified in the "Findings and Recommendations" section. Furthermore, KPMG determined the OAs failed to adequately implement and/or provide evidence of implementation

of privacy-supportive security controls to address how system privacy data is properly protected and safeguarded.

FINDINGS AND RECOMMENDATIONS

Our evaluation of the DOT and OAs PII program and practices focused on assessing the design, implementation, and operating effectiveness of the privacy controls. We identified deficiencies in three of the eight NIST privacy control areas tested during February 23, 2017 through September 20, 2017. Specifically, we identified privacy control deficiencies in AR, DM, and IP; as described in the Methodology section Table 1 above pages 7-8. These deficiencies exist because the DOT did not consistently implement and enforce PII policies and procedures in accordance with current DOT and OMB requirements.

KPMG presented the deficiencies identified as a result of our testing to the DOT. We received concurrence from the DOT prior to issuing this report.

Accountability, Audit, and Risk Management (AR) (Sub-Controls: AR-2, Privacy Impact and Risk Assessment, and AR-5, Privacy Awareness and Training)

1. Lack of Adequate Privacy Resources in place (AR-2).

Condition

During testing of FAA's selected privacy systems we noted that six (6) systems did not have fully compliant and complete Privacy Plans prior to system certification and authorization (C&A) or re-authorization. KPMG noted that some systems did have adjudicated PTAs for previous C&A cycles, but not all elements of the adjudication statement had been completed.

The incomplete privacy plan for a system may result in the inappropriate collection, use, storage, sharing, and/or loss of PII resulting in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. In addition, failure to implement the established privacy policies and/or procedures, regardless of whether the procedures are needed, greatly enhances the security and privacy risks for the Department. There is a risk that the lack of privacy plans may result in breaches occurring without being recognized, reported or addressed.

The Department requires the following to be implemented:

- The Privacy Act of 1974, as amended, is one of the key legislative acts governing the protection of records maintained on individuals. The Act (5 U.S.C. 522a) regulates the collection, maintenance, use, and dissemination of records about individuals that are retrieved by personal identifier and collected, used, or disseminated by agencies and departments. The Privacy Act also mandates the publishing of system of records notices (SORNS) for newly created and revised systems of records.
- OMB A-130 – Appendix I, Specific Requirements (Plans, controls, and Assessments – 14)). [Agencies shall] conduct and document security and privacy control assessments prior to the operation of an information system, and periodically thereafter, consistent with the frequency defined in the agency information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies and the agency risk tolerance.

- DOT Privacy Risk Management Policy – Section 18.5.2.9.2, - DOT CPO. DOT CPO approval of privacy risk management strategy is required as a precondition for the issuance of an authority to operation. The authority for selection and assessment of privacy controls ultimately rests with the Senior Agency Official for Privacy (SAOP).
- DOT Privacy Risk Management Policy – Section 18.5.6.2 – Component CIO. Ensure the Component Privacy Office is appropriately staffed and resourced.
- DOT Privacy Risk Management Policy – Section 18.5.7.7 – Coordinate Component privacy compliance documentation to ensure that the Department management, technical, and operational privacy requirements are addressed.

We recommend FAA:

1. Conduct a review of its privacy program to identify changes needed to ensure that system's privacy plans are completed in accordance with the DOT Privacy Risk Management Policy.

2. Lack of required Privacy Training in place (AR-5).

Condition

During testing of the FAA's privacy system we noted that OA management does not have specialized or role-based privacy training for personnel having responsibility for PII or for activities that involve PII. It became clear in the discussions that the privacy system personnel were not aware of what constitutes sensitive and non-sensitive PII. KPMG noted that basic training is in place and personnel are trained annually.

We also noted, from our interviews, that FAA privacy system personnel were not aware of what constitutes sensitive and non-sensitive PII. This may be due to a lack of specialized training for system personnel responsible for PII.

The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. In addition, failure to implement the established Privacy policies and/or procedures regardless of whether the procedures are needed, greatly enhances the security and privacy risks for the Department. There is a risk that the lack of formal training awareness relating to privacy issues may result in breaches occurring, but not being recognized, reported or addressed.

The Department requires the following to be implemented:

- DOT Privacy Risk Management Policy – Section 18.4.8.4.1 – Training. Agency personnel (e.g. Component Privacy Officers, program officials, information systems personnel, personnel specialists, finance officers, investigators, acquisition officials, attorneys/advisors, public affairs and disclosure officials) who maintain or have access to PII, regardless of medium, will receive specialized privacy training before being granted access to that information and/or system.

We recommend FAA:

2. Provide system specific and/or specialized/role based privacy job aides as needed to personnel who maintain and/or have access to PII data.

3. Lack of required PII documentation in place (AR-2).

Condition

During testing of the one of the FAA's privacy system, we noted that the privacy system owners did not have a fully compliant privacy plan in place.

Failure to be compliant with the privacy plan could essentially mean that the system itself is non-compliant and therefore the Senior Agency Official for Privacy may have to make a risk based decision whether to accept the non-compliant system or to cease operations until the system is compliant with the privacy plan.

In addition, failure to implement the established Privacy policies and/or procedures greatly enhances the security and privacy risks for the Department.

The Department requires the following to be implemented:

- The Privacy Act of 1974, as amended, is one of the key legislative acts governing the protection of records maintained on individuals. The Act (5 U.S.C. 522a) regulates the collection, maintenance, use, and dissemination of records about individuals that are retrieved by personal identifier and collected, used, or disseminated by agencies and departments.

- The Privacy Act also mandates the publishing of SORNs for newly created and revised systems of records.

- DOT Privacy Risk Management Policy – Section 18.5.2.9 – Establish the framework for privacy- and risk management-related reporting activities, including initiating and updating SORNs, PTAs, PIAs, SDAs and other privacy risk management and compliance documentation.

We recommend FAA:

3. Ensure the system Privacy Plan includes all requirements established by the DOT Chief Privacy Officer in the PTA and the adjudication statement is implemented.

Data Minimization and Retention (Sub-control: DM-2, Data Retention and Disposal)

4. Lack of Required PII Documentation in Place (DM-2)

Condition

During testing of the FAA's privacy system, we noted that the FAA does not have a fully compliant and approved Privacy Plan for the system. Therefore, we were unable to determine if the FAA has and is operating in accordance with an approved SORN, PIA, or NARA schedule. It was also noted during testing of FAA's privacy system that PII information is being shared with other internal systems; however, a MOU or other similar instrument documenting the purpose and conditions for sharing PII are not in place.

We also noted the FAA's privacy system does not have a Memorandum of Understanding (MOU) or other similar agreements in place for sharing of PII with other internal systems. FAA privacy system personnel may not be aware of the requirements stated in the DOT Privacy Risk Management Policy.

The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. In addition, failure to implement the established Privacy policies and/or procedures greatly enhances the privacy and security risks for the Department.

The Department requires the following to be implemented:

- The Privacy Act of 1974, as amended, is one of the key legislative acts governing the protection of records maintained on individuals. The Act (5 U.S.C. 522a) regulates the collection, maintenance, use, and dissemination of records about individuals that are retrieved by personal identifier and collected, used, or disseminated by agencies and departments.
- The Privacy Act also mandates the publishing of system of records notices SORNs for newly created and revised systems of records.
- DOT Privacy Risk Management Policy – Section 18.4.4.9 – Data Minimization and Retention. DOT will ensure that PII is disposed of, destroyed and/or erased, regardless of the storage method, in accordance with a NARA approved record retention schedule and in a manner that prevents loss, theft, misuse or unauthorized access.
- DOT Privacy Risk Management Policy – Section 18.5.2.9 – Establish the framework for privacy- and risk management-related reporting activities, including initiating and updating SORNs, PTAs, PIAs, SDAs and other privacy risk management and compliance documentation.
- DOT Privacy Risk Management Policy – Section 18.4.3.4. – Internal Sharing. DOT will document all authorized internal sharing of PII via a MOU or other approved instrument that articulates the conditions of access and use.
- DOT Privacy Risk Management Policy – Section 18.4.8.4.1 – Training. Agency personnel (e.g. Component Privacy Officers, program officials, information systems personnel, personnel specialists, finance officers, investigators, acquisition officials, attorneys/advisors, public affairs and disclosure officials) who maintain or have access to PII, regardless of medium, will receive specialized privacy training before being granted access to that information and/or system.

We recommend FAA:

4. Ensure the Privacy Plan including all requirements established by the DOT Chief Privacy Officer in the PTA adjudication statement is implemented.
5. Implement MOUs or similar agreements for internal sharing of PII.

Individual Participation and Redress (IP) (Sub-Control: IP-3, Redress)

5. PII encryption implementation inconsistencies across multiple OA's (IP-3).

Condition

During testing over the OIG's PY 2014 recommendations we noted that multiple OAs and Component systems failed to adequately implement and/or provide evidence of implementation of privacy supportive security controls. As a result, the following privacy security controls per OA and privacy system were unable to be validated due to lack of evidence:

FAA:
- Privacy System #1: Implement encryption for data at rest
- Privacy System #2: Physical drives are not configured for encryption of data at rest.

- Privacy System #3:
    - Implement encryption for data at rest; and
    - Enablement of session time-out function after 30 minutes of inactivity

OST:
- Privacy System #4:
    - Encryption for data at rest; and
    - Encryption of data during transmission.

In addition, due to the OA implementation issues identified above, KPMG determined the above privacy security controls were not continuously monitored as part of DOT's ongoing C&A process, in accordance with OMB federal requirements and DOT Privacy Risk Management Policy.

Also, OA system owners were unable to provide supporting evidence to demonstrate that privacy supportive controls were appropriately implemented by the hard stop date of August 25, 2017.

The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. In addition, failure to implement the established Privacy policies and/or procedures greatly enhances the security and privacy risks for the Department.

The Department requires the following to be implemented:

- The Privacy Act of 1974, as amended, is one of the key legislative acts governing the protection of records maintained on individuals. The Act (5 U.S.C. 522a) regulates the collection, maintenance, use, and dissemination of records about individuals that are retrieved by personal identifier and collected, used, or disseminated by agencies and departments.
- The Privacy Act also mandates agencies, "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

- DOT Privacy Risk Management Policy – Section 18.4.7.1 DOT will protect PII through appropriate security safeguards against risks such as loss; unauthorized access, use, destruction or modification; or unintended or inappropriate disclosure.
- DOT Privacy Risk Management Policy – 18.4.7.1.1. DOT will protect all records against reasonably anticipated threats or hazards that could result in harm, embarrassment, inconvenience or unfairness to any individual about whom information is maintained.

Standards

- Special Publication (SP) 800-122, Guide to Protecting the confidentiality of PII – provides listing of NIST SP 800-53 controls that can be used to help safeguard the confidentiality of PII.

We recommend OST:

6. Establish a continuous monitoring (CM) program for privacy supportive security controls to ensure PII systems remain compliant with DOT Privacy Risk Management policy.

6. Lack of required prior year PII documentation in place (IP-3).

Condition

While performing the testing over the OIG's PY recommendation #9 for a FAA privacy system #1[4], we did not receive the supporting documentation demonstrating the implementation and execution of PII security controls for the encryption of data at rest.

In addition, FAA management did not provide supporting evidence to demonstrate that encryption of data at rest is enabled on their physical drives. KPMG noted that a POAM was created on August 24, 2017 with an estimated completion date of December 19, 2017.

The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. In addition, failure to implement the established Privacy policies and/or procedures greatly enhances the security and privacy risks for the Department.

The Department requires the following to be implemented:

- The Privacy Act of 1974, as amended, is one of the key legislative acts governing the protection of records maintained on individuals. The Act (5 U.S.C. 522a) regulates the collection, maintenance, use, and dissemination of records about individuals that are retrieved by personal identifier and collected, used, or disseminated by agencies and departments.
- DOT Privacy Risk Management Policy – Section 18.4.7.1.2. – Security. At a minimum, all PII will be protected using controls consistent with Federal Information Processing Standard Publication 199 (Federal Information Processing Standards (FIPS) 199) moderate confidentially standards.
- DOT Privacy Risk Management Policy – Section 18.4.7.2. – Security. DOT will implement encryption protections, using only NIST certified cryptographic modules, for all electronic

[4] Due to privacy and sensitivity purposes, privacy system names were removed from the report.

SPII being transported and/or stored offsite unless otherwise authorized, in writing, by the DOT Deputy Secretary or a Senior DOT Official.

We recommend FAA:

7. Ensure that encryption protections for data at rest is implemented in accordance with the DOT Privacy Risk Management Policy.
8. Ensure that the Plan of Action and Milestones (POA&M) for encryption protections for data at rest is actively monitored and updated as changes occur prior to the estimated closure date of December 19, 2017.

7. Lack of required prior year PII documentation in place (IP-3).

Condition

While performing the testing over the OIG's PY recommendation #9 for a FAA privacy system #2[5], we noted that the physical drives are not configured for encryption of data at rest implementation. In addition, FAA management did not provide supporting evidence to demonstrate that encryption of data at rest is enabled on their physical drives.

The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. In addition, failure to implement the established Privacy policies and/or procedures greatly enhances the security and privacy risks for the Department.

The Department requires the following to be implemented:

The Privacy Act of 1974, as amended, is one of the key legislative acts governing the protection of records maintained on individuals. The Act (5 U.S.C. 522a) regulates the collection, maintenance, use, and dissemination of records about individuals that are retrieved by personal identifier and collected, used, or disseminated by agencies and departments.

DOT Privacy Risk Management Policy – Section 18.4.7.1.2. – Security. At a minimum, all PII will be protected using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentially standards.

DOT Privacy Risk Management Policy – Section 18.4.7.2. – Security. DOT will implement encryption protections, using only NIST certified cryptographic modules, for all electronic SPII being transported and/or stored offsite unless otherwise authorized, in writing, by the DOT Deputy Secretary or a Senior DOT Official.

We recommend FAA:

9. Ensure that the encryption protections for data at rest are implemented in accordance with the DOT Privacy Risk Management Policy.

[5] Due to privacy and sensitivity purposes, privacy system names were removed from the report.

8. Lack of required prior year PII documentation in place (IP-3).

Condition

While performing the testing over the OIG's PY recommendation #9 for a FAA privacy system #3[6], we did not receive the supporting documentation demonstrating the implementation and execution of PII security controls for the encryption of data at rest, and the enablement of session time-out functionality after 30 minutes on inactivity.

FAA privacy system owner did not provide supporting evidence to demonstrate that the encryption of data at rest or during transmission is enabled. Additionally, supporting evidence for the 30 minute session inactivity enablement was not provided.

The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. In addition, failure to implement the established Privacy policies and/or procedures greatly enhances the security and privacy risks for the Department.

The Department requires the following to be implemented:

- The Privacy Act of 1974, as amended, is one of the key legislative acts governing the protection of records maintained on individuals. The Act (5 U.S.C. 522a) regulates the collection, maintenance, use, and dissemination of records about individuals that are retrieved by personal identifier and collected, used, or disseminated by agencies and departments.

- DOT Privacy Risk Management Policy – Section 18.4.7.1.2. – Security. At a minimum, all PII will be protected using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentially standards.

- DOT Privacy Risk Management Policy – Section 18.4.7.2. – Security. DOT will implement encryption protections, using only NIST certified cryptographic modules, for all electronic SPII being transported and/or stored offsite unless otherwise authorized, in writing, by the DOT Deputy Secretary or a Senior DOT Official.

We recommend FAA:

10. Ensure that the encryption protections for data at rest and during transit are implemented in accordance with the DOT Privacy Risk Management Policy.
11. Confirm that the session time-out functionality has been implemented.

9. Lack of required prior year PII documentation in place (IP-3).

Condition

While performing the testing over the OIG's PY recommendation #9 for a FAA privacy system #4[7], we did not receive the supporting documentation demonstrating the implementation and

[6] Due to privacy and sensitivity purposes, privacy system names were removed from the report.
[7] Due to privacy and sensitivity purposes, privacy system names were removed from the report.

execution of PII security controls for the encryption of data at rest, and encryption of data during transmission.

OST privacy system owner did not provide supporting evidence to demonstrate that the encryption of data at rest or during transmission is enabled.

The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. In addition, failure to implement the established Privacy policies and/or procedures greatly enhances the security and privacy risks for the Department.

The Department requires the following to be implemented:

- The Privacy Act of 1974, as amended, is one of the key legislative acts governing the protection of records maintained on individuals. The Act (5 U.S.C. 522a) regulates the collection, maintenance, use, and dissemination of records about individuals that are retrieved by personal identifier and collected, used, or disseminated by agencies and departments.

- DOT Privacy Risk Management Policy – Section 18.4.7.1.2. – Security. At a minimum, all PII will be protected using controls consistent with FIPS 199 moderate confidentially standards.

- DOT Privacy Risk Management Policy – Section 18.4.7.2. – Security. DOT will implement encryption protections, using only NIST certified cryptographic modules, for all electronic SPII being transported and/or stored offsite unless otherwise authorized, in writing, by the DOT Deputy Secretary or a Senior DOT Official.

We recommend OST:

12. Ensure that the encryption protections for data at rest and during transit have been implemented in accordance with the DOT Privacy Risk Management Policy.

CONCLUSION

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives aforementioned above. We conclude that for the testing period February 23, 2017 through September 26, 2017, DOT has taken efforts to develop a framework for the collection, use, and security of PII data Department-wide; however DOT did not consistently implement and enforce its PII policies and procedures across its OAs in accordance with current DOT NIST, and OMB requirements. We identified nine (9) deficiencies, and twelve (12) recommendations which are listed within the “Findings and Recommendations” section of the report. These deficiencies were identified in three of the eight privacy control areas of the Department’s and OAs Implementation of PII Programs and Practices pertaining to AR, DM, and IP; as described in the Methodology section of the report pages 7-8.

The nine (9) deficiencies resulted in twelve (12) recommendations communicated to DOT management prior to the issuance of this report. The 12 recommendations are contained in Section V, Findings and Recommendations, of this report.

We also reviewed 10 prior year recommendations related to DOT's PII Policies and Procedures to determine their current status. In summary, nine (9) out of the ten (10) prior year recommendations were implemented and closed. Appendix 3, documents our review and inspection procedures performed of the DOT implementation and execution of ten recommendations made in the OIG report *Quality Controls Review for the Audit of DOT Protection of Privacy Information Report.* Appendix 2 contains a glossary of terms used in the report.

These deficiencies exist because OST and FAA did not consistently implement and enforce PII policies and procedures in accordance with current DOT and OMB requirements.

CRITERIA AND REFERENCES

KPMG considered the following criteria and references during the assessment:

Federal Laws and Regulations

1. OMB
2. The Privacy Act of 1974
3. The E-Government Act of 2002,
4. Federal Information Security Modernization Act (FISMA) of 2002
5. NIST Special Publication 800-53 Appendix J DOT Approach
6. DOT CIO Policy 1351.18, Departmental Privacy Risk Management
7. DOT CIO Policy 1351.19, PII Breach Notification Controls (NOTE: This policy is currently under review and is anticipated to be reissued as an implementation instruction under 1351.18 during Q3FY17.)
8. DOT CIO Policy 1351, Privacy Policy for the Information Sharing Environment
9. DOT Departmental Information Resource Management Manual (DIRMM), Chapter 8 Privacy Protections
10. DOT Order 1351.20, U.S. DOT Rules of Conduct and Consequences Policy Relative to Safeguarding PII
11. DOT Order 1351.37, Departmental Cybersecurity Policy
12. U.S. DOT Departmental Cybersecurity Compendium
13. U.S. DOT Biennial SORN Review Process and Guidance
14. DOT PIA Development Guide
15. Privacy Office Organizational Chart
16. Senior Agency Privacy Official Designation
17. SAOP Annual FISMA Report

APPENDIX 2

LIST OF ACRONYMS

Acronym	Definition
AR	Accountability, Audit and Risk Management
AICPA	American Institute of Certified Public Accountants
AP	Authority and Purpose
C&A	Certification and Accreditation
CIO	Chief Information Officer
CPO	Chief Privacy Officer
CM	Continuous Monitoring
DI	Data Quality and Integrity
DIRMM	Departmental Information Resource Management Manual
DM	Data Minimization and Detection
DOT	Department of Transportation
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FMCSA	Federal Motor Carrier Safety Administration
FPE	Federal Production Environment
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IP	Individual Participation and Redress
ISCM	Information Security Continuous Monitoring
MARAD	Maritime Administration
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
OAs	Operating Administrations
OIG	Office of Inspector General
OMB	Office Management and Budget
OST	Office of the Secretary
PHMSA	Pipeline and Hazardous Materials Safety Administration
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POAM	Plan of Action and Milestone
PCM	Privacy Continuous Monitoring

Acronym	Definition
PTA	Privacy Threshold Assessment
QCR	Quality Control Review
SAOP	Senior Agency Official for Privacy
SDA	System Disposal Assessments
SE	Security
SLSDC	Saint Lawrence Seaway Development Corporation
SORN	System of Records Notice
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
SSL	Secure Socket Layer
TR	Transparency
UL	Use Limitation
US	United States

APPENDIX 3

SUMMARY OF KPMG'S PRIOR YEAR OIG PII FINDINGS TO CLOSE THE QC-2014-053, QUALITY CONTROLS REVIEW FOR THE AUDIT OF DOT PROTECTION OF PRIVACY INFORMATION REPORT

The Office of the Inspector General (OIG) provided this audit report to KPMG for review and inspection. KPMG performed the below inquiry and inspection procedures, to determine whether the OIG prior year (PY) recommendations are open/closed. The table below dictates KPMG's procedures performed, and the detailed analysis is documented in KPMG's PY finding summary workpapers, provided to the OIG for review and retention. The following provides a high-level summary of KPMG's procedures performed, closure status, and summary of actions needed to close the PY findings (if applicable).

Recommendations	Inquiry procedures	Inspection procedures	Open/Closed
DOT Chief Information Officer OIG Recommendation #1 Implements and monitors a process for ensuring compliance with the Privacy Act, as amended and all other federal privacy related directives as well as DOT's established privacy and data protection policies.	• Reviewed of DOT's policy documentation to assess adherence to Section 522.	• Determined compliance with federal guidelines related to privacy and protection of personal identifiable information.	Closed
DOT Chief Information Officer OIG Recommendation #2 Implements and monitors a process for ensuring information system security controls are implemented and operating according to federal requirements and DOT policy in order to assist with safeguarding the confidentiality of PII.	• Determined whether DOT implements and monitors a process for ensuring information system security controls are implemented and operating according to federal requirements and DOT policy in order to assist with safeguarding the confidentiality of PII.	• Determined compliance with federal guidelines related to privacy and protection of personal identifiable information. • Reviewed the process to determine whether the privacy office effectively and efficiently implements and monitors system security controls ensuring they are implemented and operating according to federal requirements and DOT policy.	Closed
DOT Chief Information Officer OIG Recommendation #3	• Reviewed of DOT's Privacy Office to determine whether the office effectively and	• Reviewed the agency's organization charts/structure and interview key privacy officials to determine	Closed

Recommendations	Inquiry procedures	Inspection procedures	Open/Closed
Conducts a review of the organizational structure and resources and requests necessary changes to improve program compliance and strengthen the line of accountability from the Operating Administration Privacy programs to the Departmental Privacy officer in order for the Departmental Privacy Officer to effectively administer the implementation and management of the DOT Privacy Policy and Program.	efficiently administered DOT's privacy program. • Interviewed the Departmental Privacy Officer to determine if there a budget and sufficient resources allocated to implement and operate the organization-wide privacy program.	whether the agency has identified roles and responsibilities for key privacy officials • Determined whether the Privacy Office established processes for ensuring agency compliance with Federal and agency privacy policies. • Determined whether the Privacy Office implements procedures in identifying and securing information systems containing PII.	
<u>DOT Chief Information Officer</u> OIG Recommendation #4 Ensures the inventory of systems containing PII and DOT websites is monitored and updated at least annually and implements procedures that will trigger a change to the inventory listing when systems are added, deleted, or when changes occur.	• Determined whether DOT identified and maintained a complete inventory of information systems containing.	• Reviewed procedures related to inventory management for systems containing PII. • Reviewed procedures for DOT websites management related to PII.	Closed
<u>DOT Chief Information Officer</u> OIG Recommendation #5 Updates DOT policy to reinforce Operating Administrations responsibilities to ensure they are able to illustrate the privacy controls required by federal laws and regulations, and DOT policies by providing evidence that the controls are in place and functioning effectively and responding to	• Reviewed of DOT's policy documentation to assess updates to policies to reinforce Operating Administrations responsibilities to ensure they are able to illustrate the privacy controls required by federal laws and regulations. • Reviewed notification of findings to ensure the control weaknesses are addressed.	• Determined compliance with federal guidelines related to privacy and protection of personal identifiable information. • Determined updates are being performed to policy documentation policies to reinforce Operating Administrations responsibilities to ensure they are able to illustrate the privacy controls required by federal laws and regulations.	Closed

Recommendations	Inquiry procedures	Inspection procedures	Open/Closed
notification of findings to make sure that control weaknesses are addressed. .		• Determined notification of findings to ensure the control weaknesses are addressed.	
DOT Chief Privacy Officer OIG Recommendation #6 Conducts an annual review of DOT Privacy policies and practices to ensure policies and procedures reflect current regulations, guidance and policy.	• Reviewed of DOT's policy documentation to ensure annual reviews are being conducted.	• Determined DOT privacy policies and practices reflect the current regulations, guidance and policy.	Closed
DOT Chief Privacy Officer OIG Recommendation #7 Implements procedures that ensure oversight of PIAs, and communicates the requirements and expectations for such assessments and other activities, including but not limited to, improved recordkeeping conducted by the Operating Administration Privacy Officers necessary for program success.	• Determined whether DOT has implemented procedures requiring PIAs and has conducted PIAs for the information systems.	• For a sample of information systems, review the PIAs and determined whether these PIAs have, at a minimum, analyzed and described: • What information needs to be collected (e.g., nature and source); • Why the information is being collected (e.g., to determine eligibility); • Intended use of the information (e.g., to verify data); • With whom the information will be shared (e.g., another agency for a specified programmatic purpose); • Opportunities individuals have to decline to provide information (e.g., where providing information is voluntary) or to consent to particular uses of the information (other	Closed

Recommendations	Inquiry procedures	Inspection procedures	Open/Closed
		than required or authorized uses), and how individuals can grant consent; and • How the information will be secured (e.g., administrative and technological controls) • Perform procedures to determine whether a SORN was published in the Federal Register. • Furthermore, consistent with guidance issued by OMB in 2007 related to privacy protection (OMB Memorandum M-07-16), review procedures implemented by DOT to ensure: • Privacy is adequately protected and DOT management has implemented breach notification policies; • Procedures are in place to reduce the use of SSNs; • Policies exist to notify external agencies about privacy breaches; and • DOT has implemented policies for consequences and accountability for privacy violation.	
<u>Operating Administration Privacy Officers</u> OIG Recommendation #8 Ensure PIAs are completed, reviewed and approved by the Departmental Privacy Officer prior to the	• Determined whether PIAs are completed, reviewed and approved by the Departmental Privacy Officer prior to the deployment of any system containing PII.	• For a sample of information systems, review the PIAs and determined whether these PIAs are completed, reviewed and approved by the Departmental Privacy Officer prior to the deployment of any system containing PII.	Closed

Recommendations	Inquiry procedures	Inspection procedures	Open/Closed
deployment of any system containing PII.			
Operating Administration Privacy Officers OIG Recommendation #9 Ensure ongoing validation of specific privacy related security controls for their systems are in effect, including those that safeguard confidentiality, provide secure remote access, encryption of back up media, follow up of unauthorized mobile devices, and proper user account and password settings in accordance with DOT policy. In addition, implement procedures requiring Operating Administrations to report non-compliance in their systems to the DOT Chief Privacy Officer.	• Performed a review and analysis of DOT's network and its external websites for privacy vulnerabilities in accordance with Section 522. These privacy vulnerabilities include noncompliance with stated practices, policies and procedures as well as risks of inadvertent release of information in an identifiable form from the website of the agency. • Reviewed procedures requiring Operating Administrations to report non-compliance in their systems to the DOT Chief Privacy Officer.	• Worked with the appropriate DOT personnel to test and document the application of selected privacy related technical controls from OMB Memorandum M-06- 16, *Protection of Sensitive Agency Information,* NIST Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* and related NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* including the following: • Encryption. Encrypt, using only National Institute of Standards and Technology (NIST) certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or a senior-level individual he/she may designate in writing; • Control Remote Access. Allowed remote access only with two-factor authentication where one of the factors is provided by a device separate from the	Open, Findings #6, 7, 8, and 9.

Recommendations	Inquiry procedures	Inspection procedures	Open/Closed
		computer gaining access; • Time-Out Function. Use a "time-out" function for remote access and mobile devices requires user re-authentication after thirty minutes of inactivity; • Log and Verify. Logged all computer-readable data extracts from databases holding sensitive information and verified each extract, including whether sensitive data has been erased within 90 days or its use is still required; and • Ensure Understanding of Responsibilities. Ensured all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities. • performed procedures to determine if the Agency has implemented encryption on data transmitted over the agency's communication infrastructure with emphasis on encryption of systems containing privacy data. • for a sample websites to determined the following: • Determined whether the website is using Secure Socket Layer (SSL) to capture and	

Recommendations	Inquiry procedures	Inspection procedures	Open/Closed
		transfer Privacy Act protected user data.	
Operating Administration Privacy Officers OIG Recommendation #10 Conduct an annual review their web sites ensuring proper and accurate posting of their Privacy policies.	• Gained an understanding of the DOT's documented standards regarding its system's handling and tracking of PII for DOT websites.	• Determined if procedures are in place to conduct annual reviews of websites. • Determined whether the appropriate privacy policy and disclosures are posted and available for all visitors and users of the website. In addition, assess the web privacy policies to determine compliance with the requirements set forth in OMB Memorandum M-03-22, Section III – *Privacy Policies on Agency Websites*, and DOT Privacy Policies. • Determined whether the website is in compliance with the use of tracking mechanisms. • Determined whether DOT has implemented machine readability technology on its public website, such as Privacy Preferences Project Protocol (P3P).	Closed

U.S. DOT OIG

Fraud & Safety Hotline

hotline@oig.dot.gov | (800) 424-9071

https://www.oig.dot.gov/hotline

Our Mission

OIG conducts audits and investigations on behalf of the American public to improve the performance and integrity of DOT's programs to ensure a safe, efficient, and effective national transportation system.

OFFICE OF INSPECTOR GENERAL
U.S. Department of Transportation
1200 New Jersey Ave SE
Washington, DC 20590

www.oig.dot.gov