Office of Inspector General
Audit Report

QUALITY CONTROL REVIEW FOR THE AUDIT OF DOT PROTECTION OF PRIVACY INFORMATION

Department of Transportation

Report Number: QC-2014-053
Date Issued: June 05, 2014

Memorandum

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

Subject: ACTION: Quality Control Review for the Audit of DOT Protection of Privacy Information
Report Number QC-2014-053

Date: June 5, 2014

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

Reply to Attn. of: JA-20

To: Chief Information Officer

The Department of Transportation (DOT) works to protect the privacy of all individuals while delivering efficient, accessible, and convenient transportation systems and services. Through its privacy program, DOT has determined that 167 of its 454 computer systems contain personally identifiable information (PII) about the public and/or DOT employees. Eleven of DOT's 12 operating administrations have at least one system with privacy information.

In the Fiscal Year 2005 Consolidated Appropriations Act for Transportation, Treasury, Independent Agencies, and General Government,[1] Congress required agencies to enhance the protection of PII that they collect and use. The act also required agencies to create Chief Privacy Officer positions, submit reports on their privacy programs to Congress and their inspectors general, and have independent third-party audits of their privacy programs performed.

Our 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) operating administrations properly evaluate the necessity of using PII to process system data.

We contracted with an independent auditor, CliftonLarsonAllen LLP (CLA), to conduct this work. CLA concluded that the privacy controls tested, taken collectively, were not effective and made ten recommendations to improve DOT's

[1] Pub. L. 108-447, Div. H, Title V, § 522 (December 8, 2004), as amended by Pub. L. 110-161, Div. D, Title VII, § 742(b) (December 26, 2007).

privacy program which are included in this report's exhibit.[2] We agree and are not making any additional recommendations. As of May 9, 2014, DOT's Chief Privacy Officer concurred with the recommendations and committed to the completion of corrective actions (see the appendix to this report). In accordance with DOT Order 8000.1C, the corrective actions taken in response to the findings are subject to follow-up.

We performed a quality control review (QCR) of CLA's report 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 protection of privacy information. CLA is responsible for its independent auditor's report, dated March 24, 2014, and the conclusions expressed in that report (see attachment). Our QCR disclosed no instances in which CLA did not comply, in all material respects, with generally accepted Government auditing standards.

We appreciate the courtesies and cooperation of the representatives of DOT and its operating administration representatives during this engagement. If you have any questions concerning this report, please call me at (202) 366-1407, or Nathan Custer, Program Director, at (202) 366-5540.

Attachments

#

cc: Deputy Secretary
DOT Chief Information Officer's Council Members
DOT Audit Liaison

[2] For security reasons, specific information concerning privacy program weaknesses, vulnerabilities, and deficiencies are not discussed in this report but were provided to DOT and operating administrations' privacy officers.

EXHIBIT. RECOMMENDATION SUMMARY OF CLA LLP, INDEPENDENT AUDITOR

CLA made the following recommendations, and OIG agrees, that DOT should implement to enhance its privacy program controls.

DOT Chief Information Officer	
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 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 notification of findings to make sure that control weaknesses are addressed.
DOT Chief Privacy Officer	
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 Operating Administration Privacy Officers necessary for program success.
Operating Administration 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 Operating Administrations to report non-compliance in their systems to the DOT Chief Privacy Officer.
10	Conduct an annual review their web sites ensuring proper and accurate posting of their Privacy policies.

Appendix

See the next page for Agency Comments.

TO: Louis King
Assistant Inspector General for Financial and
Information Technology Audits

FROM: Richard McKinney
Chief Information Officer (CIO)

May 9, 2014

SUBJECT: ACTION: Response to the Office of Inspector General
Draft Report on US Department of Transportation's Privacy Program and
Implementation - 2013

The Department of Transportation (DOT) continues to strengthen the primary mission of the privacy program, which is to protect and educate all individuals impacted by our work activities, as well as respect the needs of our employees. There are privacy elements to every aspect of the collection, maintenance, disclosure, and destruction of information about individuals; either collected, used, or created by DOT. We acknowledge the continuing challenge to institutionalize a culture of privacy within all of our employees. The Department also recognizes that these challenges, and the safeguarding of its vast information holdings, are only successful through a shared understanding and practice of all employees.

In the ongoing efforts to move the program forward, the DOT Chief Privacy Officer (CPO} drafted a comprehensive policy that addresses Privacy at the Department. The draft DOT Privacy Risk Management Policy, received significant contributions from privacy, security, information management and legal professionals across the Department. The policy is expected to be submitted for final concurrence and signature in September 2014 and will firmly establish the Department's privacy framework. Centered on the Fair Information Practice Principles (FIPPs}, the policy will clarify compliance requirements and responsibilities. Once the policy is published, the DOT CPO will issue supplemental guidance and implementation instructions necessary to ensure consistent and verifiable execution of policy requirements, roles, and responsibilities.

RECOMMENDATIONS AND RESPONSE

Recommendation 1: Conduct an annual review of DOT Privacy policies and practices to ensure policies and procedures reflect current regulations, guidance and policy.

Response: Concur. The DOT CPO will conduct an annual review of the forthcoming Privacy Risk Management Policy upon its issuance anniversary. The review will address any gaps in coverage or implementation and will be updated accordingly. Expected completion date is September 30, 2015.

Recommendation 2: Implement 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 (OA} Privacy Officers necessary for program success.

Response: Concur. The DOT CPO will issue supplemental guidance and implementation instructions to the forthcoming DOT Privacy Risk Management Policy that address the requirements and expectations for the timely completion, acceptance and publication of PIAs. The supplemental guidance and implementation instructions will articulate when activities must be completed and the timing of any required reviews, updates, and approvals by the DOT CPO. Expected completion date is December 31, 2014.

Recommendation 3: Ensure PIAs are completed, reviewed and approved by the Departmental Chief Privacy Officer prior to the deployment of any system containing PII.

Response: Concur. The DOT CPO will issue supplemental guidance and implementation instructions to the forthcoming DOT Privacy Risk Management Policy to include specific requirements for the completion of privacy risk assessment documentation. The supplemental guidance and implementation instructions will clearly articulate when assessment activities must be completed and the timing of any required reviews, updates, and approvals by the DOT CPO. OA Privacy Officers remain responsible for ensuring the execution of privacy risk management activities within their OA. Expected completion date is December 31, 2014.

Recommendation 4: Ensure the inventory of systems containing PII and DOT websites are 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.

Response: Concur. The DOT CPO and the Director of Information Technology (IT) Strategy will review the existing processes for updating and maintaining the DOT website inventory. The review will be used to identify means of improving the efficiency and effectiveness of website management and oversight activities. Expected completion date is March 30, 2015.

Recommendation 5: Implement and monitor 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.

Response: Concur. The DOT CPO will review the security controls included in NIST 800-53r4 and identify those controls which directly support the forthcoming DOT Privacy Risk Management Policy. The DOT CPO will determine which of these privacy supporting security controls should be implemented by systems that collect, use, store, or transmit sensitive PII and work the Chief Information Security Officer (CISO) to develop an approach for their incorporation into the Department's existing continuous monitoring program. If necessary, the DOT CPO will issue supplemental guidance and implementation instruction(s) for the forthcoming DOT Privacy Risk Management Policy for continuous monitoring of privacy supporting security controls. Expected completion date is March 30, 2015.

Recommendation 6: 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.

Response: Concur. The DOT CPO will issue supplemental implementation instructions to the forthcoming DOT Privacy Risk Management Policy requiring OAs to verify the implementation of the controls cited (safeguarding confidentiality, provide secure remote access, encryption of back-up media, follow-up of

Unauthorized mobile devices, and proper user account and password settings) for all systems containing sensitive PII. The implementation instructions will require OAs to report compliance gaps to the CPO and CISO, enter Plans of Actions & Milestones (POA&M) into the Cyber Security Assessment and Management (CSAM) system, and keep the CPO and CISO apprised of progress in closing POA&Ms. Expected completion date is March 30, 2015.

Recommendation 7: Conduct an annual review their web sites ensuring proper and accurate posting of their Privacy policies.

Response: Concur. The forthcoming DOT Privacy Risk Management Policy will clarify requirements for OAs implementation and periodic review of their websites. The DOT CPO will conduct an annual review of OAs to ensure they have an approved website privacy policy, and address any compliance gaps. Expected completion date is September 30, 2014.

Recommendation 8: Conduct 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 DOT Privacy Officer to effectively administer the implementation and management of the DOT Privacy Policy and Program.

Response: Concur. The DOT CIO will conduct a review of the organizational structure and resources allocated to the privacy risk management program and recommend necessary changes to ensure that the DOT privacy program is appropriately organized and adequately resourced to meet its obligations. The review will include a comparison of the privacy program structure, roles, responsibilities, and resources with those of similar federal agencies. Expected completion date is December 31, 2014.

Recommendation 9: Implement and monitor 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.

Response: Concur. The forthcoming Risk Management Policy will address DOT and OA responsibilities for compliance with the Privacy Act, other federal statute, guidance, and other DOT policy. The DOT CPO will issue supplemental guidance and implementation instructions to the forthcoming policy to include specific requirements for ensuring appropriate implementation and monitoring of compliance with the Privacy Act and other federal privacy related directives and DOT policy as appropriate. The guidance and implementation instructions will clearly articulate when assessment activities must be completed and the timing of any required reviews, updates, and approvals by the DOT CPO. OA Privacy Officers remain responsible for ensuring the execution of privacy risk management activities within their OA. Expected completion date is September 30, 2014.

Recommendation 10: Update 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 notification of findings to make sure that control weaknesses are addressed.

Response: Concur. The forthcoming Privacy Risk Management Policy will address DOT and OA responsibilities for compliance with the Privacy Act, other federal statute, guidance, and other DOT policy. The DOT CPO will issue supplemental guidance and implementation instructions to the forthcoming policy to include specific requirements documenting evidence of implementation and on-

going management of privacy controls. The guidance and implementation instructions will establish baseline controls to be implemented by OAs. The guidance and instructions will clearly articulate when controls must be implemented and the timing of any required reviews, updates, and approvals by the DOT CPO. OA Privacy Officers remain responsible for ensuring the execution of privacy risk management activities within their OA. Expected completion date is September 30, 2014.

The Office of the DOT CIO appreciates the opportunity to review and respond to the report. If you have any questions concerning the response, please contact Claire Barrett at (202) 527.3284, or by email at claire.barrett@dot.gov

Attachment

See the next page for the Independent Auditor’s Report.

CliftonLarsonAllen LLP
www.claconnect.com

CliftonLarsonAllen LLP's Independent Audit of the Department of Transportation's Privacy Program and Implementation - 2013

Prepared for the
Assistant Inspector General for
Financial and Information Technology Audits
Department of Transportation
Office of Inspector General

March 24, 2014

Table of Contents

Executive Summary

March 24, 2014

Office of Inspector General
Department of Transportation
1200 New Jersey Ave, SE
Washington, DC 20590

Section 522 of the Consolidated Appropriations Act of 2005, (Division H, Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005) as amended requires that each agency designate a Chief Privacy Officer (CPO) and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to agency employees and the public. Section 522 also requires the Inspector General of each agency to periodically conduct a review of the agency's implementation of the requirements of Section 522 including the agency's privacy program. The Department of Transportation Office of the Inspector General (DOT-OIG) contracted with CliftonLarsonAllen (CLA) to conduct a review of the DOT information management practices for protection of Personally Identifiable Information (PII), as they relate to the guidelines set forth in the Section 522 of the Consolidated Appropriations Act of 2005. In this section of the Act, the definition of "identifiable form" is consistent with Public Law 107-347, the E-Government Act of 2002, and means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

The objective of the audit was to evaluate DOT information management practices for the protection of PII in order to:

A. determine the accuracy of the descriptions of the use of information in identifiable form while accounting for current technologies and processing methods;
B. determine the effectiveness of privacy and data protection procedures by measuring actual practices against established procedural guidelines;
C. ensure compliance with the stated privacy and data protection policies of DOT and applicable laws and regulations; and
D. ensure that all technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in operation of the program and provide DOT with recommendations, strategies, and specific steps, to improve privacy and data protection management.

CLA's audit included interviewing key privacy personnel and a review of DOT's privacy related policies and procedures including incident response, the structure and positioning of the Privacy Office's function within the agency, the monitoring and compliance efforts of the Privacy Office, DOTs technical controls to protect privacy information, review of DOT's website compliance and review of DOT's privacy related training program. These areas were assessed accordingly within the context of the requirements and recommendations of Section 522 of the Consolidated Appropriations Act of 2005, Section 208 of the E-Government Act of 2002, the Privacy Act of 1974, Office of Management and

Budget (OMB) Memorandum M-00-13, M-03-22, M-05-08, M-06-19, M-07-16, M-10-22 and M-99-18, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122. Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS).

DOT has determined that 167 systems of its 454 computer systems contain personally identifiable information (PII) about the public and DOT employees. Twelve of the thirteen Operating Administrations (OAs) contained at least one system with privacy information. DOT's privacy program had a number of strengths, including but not limited to the following:

- Privacy reporting activities met the requirements of OMB and the E-Government Act of 2002;
- The Breach Notification Policy is documented and roles and responsibilities are defined;
- Privacy incidents are tracked and reported in compliance with United States Computer Emergency Readiness Team (US-CERT) timelines; and
- Individuals with increased privacy responsibilities complete specialized privacy training on an annual basis

While DOT's privacy program had a number of strengths, DOT needs to strengthen its implementation of information privacy protections, including full compliance with federal laws, regulations and policies. The audit identified the following opportunities for improving the overall agency-wide privacy program:

- DOT privacy protection policies need to be enhanced;
- The process of completing Privacy Impact Assessments (PIAs) needs improvement;
- The process of regularly monitoring and updating the DOT website inventory needs improvement;
- Technology controls to assist in safeguarding the confidentiality of PII need improvement;
- The process of regularly reviewing the privacy policy content on DOT websites needs improvement;
- The current organizational structure needs to be reviewed to ensure effective management and accountability of the privacy program; and
- Management needs to demonstrate that controls are effectively implemented for safeguarding PII. In addition, management needs to respond to notification of control weaknesses.

Further, several of the recommendations made in this report relate to privacy practices that have not been incorporated into the agency's policies and procedures. Absent formal policies and procedures, DOT cannot ensure consistent program implementation. In addition, there may be potential civil and criminal ramifications associated with noncompliance with laws if agency employees do not understand their responsibilities under the various privacy laws. DOT is vulnerable to an increased risk of a breach of sensitive data, which may result in personal harm, loss of public trust, legal liability, or increased costs of responding to a breach. Addressing these control deficiencies in privacy and data protection procedures will strengthen DOT's privacy program and contribute to ongoing efforts to achieve reasonable assurance of adequate protection of PII. This report makes ten recommendations to assist DOT in strengthening its privacy program.

CLA concluded that the privacy controls tested taken collectively were not effective. This performance audit did not constitute an audit of financial statements in accordance with GAGAS. CLA was not engaged to, and did not render an opinion on the DOT's internal controls over financial reporting or

financial management systems. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that controls may become inadequate because of changes in conditions, or because compliance with controls may deteriorate.

Sincerely,

CLIFTONLARSONALLEN LLP

Background

On October 15, 1966 the Department of Transportation was established by an act of Congress. The mission of the Department is to serve the United States by ensuring a fast, safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people, today and into the future. During the audit period the Department consisted of the Office of the Secretary, the Office of the Inspector General and eleven other Operating Administrations (OAs): the Federal Aviation Administration (FAA), the Federal Highway Administration (FHWA), the Federal Motor Carrier Safety Administration (FMCSA), the Federal Railroad Administration (FRA), the National Highway Traffic Safety Administration (NHTSA), the Federal Transit Administration (FTA), the Maritime Administration (MARAD), the Pipeline and Hazardous Materials Safety Administration (PHMSA), the Research and Innovative Technology Administration (RITA),[1] the Saint Lawrence Seaway Development Corporation (SLSDC), and the Surface Transportation Board (STD). The Department had a $147.6 million budget for fiscal year 2013 and a staff of more than 57,000.

The Department of Transportation Office of the Inspector General contracted with CliftonLarsonAllen (CLA) to conduct a review of DOT's information management practices for protection of Personally Identifiable Information (PII), as they relate to the guidelines set forth in Section 522-d of the Consolidated Appropriations Act of 2005.

Public Law No. 108-447, Division H, Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005 (commonly referred to as the Consolidated Appropriations Act of 2005) and OMB Memorandum M-05-08 Designation of Senior Agency Officials for Privacy states that each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy. According to Section 522, each agency shall prepare a written report of its use of information in an identifiable form,[2] along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Examples of information in identifiable form, also referred to as personally identifiable information include name, address, social security number (SSN) or other identifying number or code, telephone number, email address, etc. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report.

In addition, Section 522 requires the Inspector General of each agency to periodically conduct an independent third party review of the agency's implementation of the requirements of the section to include:

- Evaluating the agency's use of information in identifiable form;
- Evaluating the privacy and data protection procedures of the agency; and
- Recommending strategies and specific steps to improve privacy and data protection management.

[1] On January 30, 2014 The Department of Transportation's Research and Innovation Technology Administration (RITA) was integrated into DOT's Office of the Secretary of Transportation (OST) under the new name of the Office of the Assistant Secretary for Research and Technology. The Research and Technology team now reports directly to the DOT Secretary as part of the Omnibus bill signed by President Obama earlier in January 2014 elevating research, innovation and technology within DOT.

[2] The definition of "identifiable form" is consistent with the E-Government Act of 2002 (Public Law No. 101-347), and means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct of indirect means.

Per the requirements above, the independent third party review must also include:

- 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;
- 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;
- A detailed analysis of agency intranet, 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; and
- A review of agency compliance with Section 522.

The Privacy Act of 1974, 5 U.S.C. § 552a, as amended, and OMB Memorandum M-06-15 Safeguarding Personally Identifiable Information, 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.

DOT Privacy Office

DOT collects and uses a significant amount of PII of both employees and the public. The DOT Privacy Office is staffed by four employees. The goal of the DOT Privacy Program is the protection of PII. The program provides leadership and assistance to DOT's OAs on issues related to the Privacy Act of 1974, E-Government Act of 2002 and related Office of Management and Budget privacy guidance. The Chief Information Officer (CIO) has been designated as the Senior Agency Official for Privacy and is responsible for the DOT Privacy Policy and Program and for providing guidance to DOT supervisors and employees concerning the implementation and application of the Privacy Act, as amended. The Departmental Privacy Officer is the individual appointed by the Chief Information Officer responsible for overseeing the implementation and management of the DOT Privacy Policy and Program. Two staff report to the Departmental Privacy Officer including an employee from OST and an FAA detailee providing assistance 20% of the time. Additionally, each OA is comprised of a Privacy Officer. The OA Privacy Officer is responsible for coordinating privacy-related activities and providing guidance on privacy issues within their organizations and implementing privacy policies and procedures within the OA, in coordination with the Departmental Privacy program. The DOT privacy officer maintains an inventory of all

information technology systems that collect, use, and share public or employee PII. As of the date of this report, there are 167 such systems. Twelve of the thirteen Operating Administrations contained at least one system with privacy information. The FAA, FMCSA, and OST maintain the largest number of PII systems.

DOT Privacy Monitoring and Compliance

DOT's policy requires the Departmental Privacy Officer to evaluate the effectiveness of DOT's compliance with the Privacy Act, as amended, to ensure the Department is in full compliance with the law and all relevant directives. These duties include overseeing the Privacy Impact Assessment (PIA) process to ensure all DOT information programs address and resolve privacy issues including renewing/revising PIAs when there are changes, but not less often than every three years. According to OMB a PIA is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The system owner completes the PIA in coordination with the OA Privacy Officer and the Departmental Privacy Officer reviews and adjudicates the PIA. In addition, the Departmental Privacy Officer is responsible for reviewing, every two years, system of records notices for the Department for accuracy and ensuring amended notices are published to the Federal Register.

DOT Privacy Awareness and Training

According to DOT policy, all DOT employees who come in contact with personal information and the systems that manage that information are required to be aware of legal and Departmental requirements. Training is developed by each OA's Privacy Officer on a yearly basis. Individuals with increased privacy responsibility complete specialized privacy training each year.

The DOT specialized training program for the Chief Information Security Officer, the Information System Security Manager, the information owner, and the staff that supports the responsibilities of these individuals may include the Certified Information Privacy Professional (CIPP) and Certified Information Privacy Professional/ Government (CIPP/G). The Information System Security Officer, the System Administrator, Software Developer/ Programmer, Help Desk Coordinator, Database Administrator and Network Administrator training may include the Certified Information Privacy Professional/Information Technology (CIPP/IT).

Results of Audit

Overview

A comprehensive privacy program helps to ensure that risks related to the collection, storage, transmission and destruction of PII are mitigated. A strong privacy program also provides a framework for the agency to consider the implications of business decisions made as they pertain to PII. A privacy program should also help maintain public trust and confidence in an organization, protect the reputation of an organization, and protect against legal liability for an organization by providing the necessary safeguards to minimize the risk of unintended disclosure of PII.

DOT's privacy program had a number of strengths, including but not limited to the following:

- Privacy reporting activities met the requirements of OMB and the E-Government Act of 2002;
- The Breach Notification Policy is documented and roles and responsibilities are defined;
- Privacy incidents are tracked and reported in compliance with USCERT timelines; and
- Individuals with increased privacy responsibilities complete specialized privacy training on an annual basis.

While DOT's privacy program had a number of strengths, DOT needs to strengthen its implementation of information privacy protections, including full compliance with federal laws, regulations and policies. The audit identified the following opportunities for improving the overall agency-wide privacy program:

- DOT privacy protection policies need to be enhanced;
- The process of completing Privacy Impact Assessments needs improvement;
- The process of regularly monitoring and updating the DOT website inventory needs improvement;
- Technology controls to assist in safeguarding the confidentiality of PII need improvement;
- The process of regularly reviewing the privacy policy content on DOT websites needs improvement;
- The current organizational structure needs to be reviewed to ensure effective management and accountability of the privacy program; and
- Management needs to demonstrate that controls are effectively implemented for safeguarding PII. In addition, management needs to respond to notification of control weaknesses.

Further, several of the recommendations made in this report relate to privacy practices that have not been incorporated into the agency's policies and procedures. Absent formal policies and procedures, DOT cannot ensure consistent program implementation. Addressing these control deficiencies in privacy and data protection procedures will strengthen DOT's privacy program and contribute to ongoing efforts to achieve reasonable assurance of adequate protection of PII. This report makes ten recommendations to assist DOT in strengthening its privacy program.

CLA concluded that the privacy controls tested taken collectively were not effective. This performance audit did not constitute an audit of financial statements in accordance with GAGAS. CLA was not engaged to, and did not render an opinion on the DOT's internal controls over financial reporting or financial management systems. Furthermore, the projection of any conclusions, based on our findings,

to future periods is subject to the risk that controls may become inadequate because of changes in conditions, or because compliance with controls may deteriorate.

Appendix II (page 26) of this report summarizes the results of testing performed of key criteria selected for evaluation associated with DOT's privacy program and its implementation. Our detailed findings are discussed on pages 11-20.

Finding 1. DOT Privacy Protection Policies Need to be Enhanced

The Privacy Act of 1974 requires each agency head to establish and maintain procedures to establish reasonable administrative, technical, and physical safeguards to assure that records are disclosed only to those who are authorized to have access and otherwise 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.

We noted certain key privacy criteria was not fully addressed in the Departmental Information Resources Management Manual (DIRMM) such as the reduction of social security numbers; and logging of data extracts holding sensitive information and erasing sensitive data within 90 days unless still required. The Departmental Privacy Officer recognized the need for updating the DOT privacy policy and procedures and drafted an updated policy, DOT Order 1351.XX *Privacy Risk Management*. The draft policy is in process of being reviewed by the OA privacy officers and CIOs. The final policy will require inter-agency concurrence which is planned for the third quarter of 2014. The Draft policy addresses making reasonable attempts to substitute other identifying information in place of collecting SSNs. Although the Draft policy discusses certain security requirements it does not specifically address privacy requirements regarding data extracts.

The purpose of these policies and procedures is to define the agency-wide privacy program and practices. Without comprehensive up-to-date privacy policies and procedures, there is an increased likelihood that privacy may not be fully addressed throughout the lifecycle of DOT's information systems. Moreover, employees and contractors may be performing tasks without clear direction or training, potentially increasing the risk that PII may become subject to unauthorized access, resulting in improper handling or abuse of information.

We recommend the DOT Departmental Privacy Officer:

Recommendation #1. Conducts an annual review of DOT Privacy policies and practices to ensure policies and procedures reflect current regulations, guidance and policy.

Finding 2. DOT needs to improve the process of conducting Privacy Impact Assessments (PIAs)

The E-Government Act requires agencies to conduct a PIA for systems that collect, maintain or disseminate information in identifiable form from or about members of the public[3], or when initiating a new electronic collection of information in identifiable form for 10 or more persons. The PIA is to be reviewed by the Chief Information Officer, or equivalent official; and if practicable, the privacy impact assessment is to be publicly available through the website of the agency, publication in the Federal Register, or other means. Furthermore, OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* states that Privacy Impact Assessments should be conducted as part of the continuous monitoring program for assessing management, operational and technical controls used to safeguard information systems. Additionally, The Privacy Act

[3] According to the OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* information in identifiable form is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

requires a system of records notice to be published in the Federal Register when an agency establishes a group of records from which information in identifiable form is retrieved.[4]

According to DOT policy, the Departmental privacy officer is responsible for overseeing the Privacy Impact Assessment process to ensure all DOT information programs address and resolve privacy issues and renewing/revising privacy impact assessments when there are changes, but not less often than every three years. Operating Administration Privacy Officers are responsible for coordinating privacy-related activities and providing guidance on privacy issues within their organizations and implementing privacy policies and procedures within the OA, in coordination with the Departmental Privacy program. DOT policy also requires prior to using a record, system owners, with the assistance of their OA Privacy Officer (or the Departmental Privacy Officer for OST offices) must verify that the intended activity is listed as a routine use in the System of Records notice published in the Federal Register (if a Privacy Act system of records). The general public is to be notified of DOT's systems of personal information records through notice in the Federal Register, in compliance with the Privacy Act.

Based on our review of the September 9, 2008 *Review of DOT Privacy Policies and Procedures* report and our audit results, we noted that DOT has not made improvements in completing PIAs for information systems containing PII. In 2008, the privacy review reported that one from a sample of 20 systems did not have a completed PIA. Current audit results show that from a sample of 17 systems tested, 11 did not have a completed PIA showing a decline in DOT's management of the PIA process over the last five years. We also noted that four from the sample of 17 PIAs were not reviewed and updated within the last three years as required by DOT policy. Furthermore, a SORN was not created and published in the Federal Register for one system tested. Without completing a PIA on a system with PII, DOT may face a potential loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of PII.

Furthermore, OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* dated May 22, 2007 directed agencies to review their use of social security numbers (SSNs) in agency systems and programs to identify instances in which collection or use of the social security number is superfluous. Within 120 days from the date of this memo, agencies were to establish a plan in which the agency would eliminate the unnecessary collection and use of social security numbers within eighteen months. DOT management stated the PIA documentation and biennial System of Records Notice (SORN) review processes is the established plan for reviewing the use of social security numbers in DOT systems and programs and eliminating the unnecessary collection and use of SSNs. As a result of the ineffective management of the current PIA process resulting in the lack of documented and periodic review of PIAs, DOT is at increased risk of not complying with the OMB directive to review the use of SSNs in agency systems and programs and eliminate the unnecessary collection and use of SSNs.

The OA Privacy Officers did not coordinate the privacy-related activities associated with conducting the PIA as required by DOT policy. We also noted a lack of coordination and inconsistent record keeping between the FAA Privacy Officer and the Departmental Privacy Officer with regard to the status of the FAA PIAs. In addition, due to the increased rigor and quality of the review PIAs are subject to by the Departmental Privacy Officer, the time between submission of PIAs for review and publication has

[4] According to Public Law 93-579, as codified at 5 U.S.C. 552a, The Privacy Act (as amended) a "system of records" means a group of any records under the control of any agency 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.

increased for some systems. The Departmental Privacy Officer has noted incomplete or inconsistent information in the PIAs. Increased attention to detail and quality by the OA Privacy Officers in documenting the PIAs would reduce the number of comments from the Departmental Privacy Officer that are required to be addressed after initial submission. We noted that a PIA Guidance document has been drafted and circulated with the Operating Administrations by the Departmental Privacy Officer. The PIA Guidance will be finalized and released after the publication of the DOT Order on Privacy Risk Management.

We recommend the DOT Departmental Privacy Officer:

Recommendation #2. 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.

We recommend the Operating Administration Privacy Officers:

Recommendation #3. Ensure PIAs are completed, reviewed and approved by the Departmental Privacy Officer prior to the deployment of any system containing PII.

Finding 3. DOT needs to improve the process of regularly monitoring and updating the DOT website inventory

The E-Government Act and OMB guidance requires agencies to post privacy policies on agency websites used by the public. In order to effectively manage privacy policy information on agency websites, an accurate inventory of agency websites is necessary. Based on our review of the inventory of DOT websites provided by the Departmental Privacy Officer, we noted the inventory listing was not accurate to account for all current websites. For example, two FHWA websites on the inventory listing were not functioning. FHWA management confirmed the information was transferred to new websites due to reconstruction of the websites. However, the two new websites were not listed in the website inventory list.

NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (PM-5), Information System Inventory, requires organizations to develop and maintain an inventory of its information systems. The DOT Chief Information Officer did not provide the oversight required to ensure DOT components updated and maintained the inventory of DOT websites.

Without an accurate inventory listing of DOT websites, DOT may not be aware of all agency websites that collect PII. Consequently, DOT may be exposed to inappropriate or unauthorized access of PII which may result in personal harm, loss of public trust, legal liability or increased costs of responding to a breach of PII.

We recommend the DOT Chief Information Officer:

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.

Finding 4. DOT needs to improve technology controls to assist in safeguarding the confidentiality of PII

The Privacy Act of 1974 and the Consolidated Appropriations Act of 2005 require appropriate safeguards to ensure the security and confidentiality of records and to protect information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The Consolidated Appropriations Act of 2005 specifies that the Chief Privacy Officer is to assume primary responsibility for privacy and data protection policy, including assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form and ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

NIST SP 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* describes many types of security controls available to safeguard the confidentiality of PII including identification and authentication, allowing remote access only with two-factor authentication and using a time-out function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity, and encryption of remote access communications and removable information system media in transport and in storage.

We noted the following issues related to security controls for safeguarding the confidentiality of PII:

- DOT needs to strengthen controls for remote access
- DOT needs to ensure password configurations for all systems are in compliance with DOT policy
- DOT needs to ensure encryption of all removable media containing PII
- DOT needs to enhance the monitoring process of unauthorized mobile devices

<u>Remote Access</u>

OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, requires that Federal agencies must implement protection of "Remote" Information for the protection of PII. Remote access pertains to information accessed remotely or physically transported outside of the agency's secured, physical perimeter (this includes information transported on removable media and on portable/mobile devices such as laptop computers and/or personal digital assistants). This guidance specifies that agencies implement NIST Special Publication (SP) 800-53 security controls enforcing encrypted remote access sessions and encrypted remote storage of personally identifiable information. The specific intent for the requirements is to compensate for the protections offered by the physical security controls when information is removed from, or accessed from outside of the agency location. Furthermore OMB Memorandum M-06-16 requires organizations to allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access; and to use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity.

DOT policy adheres to NIST and OMB requirements by requiring System Owners to enforce multi-factor authentication for all network access to privileged and non-privileged accounts. All remote devices which require remote access to a DOT network or system must implement a time-out function for remote access that requires a user to re-authenticate after no more than 30 minutes of inactivity. However, we were not able to validate that this control was implemented due to lack of evidence provided.

In addition, based on review of the FY 2013 Department of Transportation FISMA report issued November 22, 2013, we noted that DOT has made limited progress in implementing the use of Personal Identification Verification (PIV) cards for user access to systems. During 2012, DOT increased PIV card issuance to above 97 percent, but provisioning (unique identifiers that associate a card to its holder) remains at only 13 percent. Therefore, the implementation of two-factor authentication for remote access has not been fully implemented.

Finally, we were not able to validate whether remote access to the MARAD system tested was encrypted due to lack of evidence provided.

Password Configuration

NIST SP 800-53, IA-2, Identification and Authentication (Organizational Users), requires information systems to uniquely identify and authenticate organizational users. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Also, IA-5, Authenticator Management requires that user authenticators such as passwords have sufficient strength for their intended use. The information system should support user authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length and password composition.

We noted the following exceptions related to non compliance with DOT policy for password configuration:

- From a sample of 10 FAA systems tested, three systems were not in compliance with DOT policy.
- For the sample of one FMCSA system tested, the system was not in compliance with DOT policy.
- For the sample of one MARAD system tested, the system was not in compliance with DOT policy.
- For the sample of one NHTSA system tested, the system was not in compliance with DOT policy.
- From a sample of two OST systems tested, one system was not in compliance with DOT policy. For the other system we were not able to determine whether the system was in compliance with DOT policy due to lack of evidence provided.
- For the sample of one RITA system tested, the system was not in compliance with DOT policy.

Based on our review of the September 9, 2008 *Review of DOT Privacy Policies and Procedures* report and our current audit test results, we noted an increase in DOT systems that were not compliant with DOT password configuration policy in the last five years. In the 2008 privacy review, four from a sample of 20 systems were not in compliance; current audit results showed that nine from a sample of 17 systems were not in compliance.

Encryption of Backup Media

NIST SP 800-53, MP-4, Media Storage, requires organizations to protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. MP-5, Media Transport requires organizations to protect and control media during transport outside of controlled areas. The supplemental guidance states that physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the

information residing on the media, and consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

In addition, DOT policy states the system owner must protect the confidentiality and integrity of backup information at the storage location. All sensitive data stored on media must be encrypted using FIPS 140-2 encryption standards. Furthermore, the DOT Rules of Behavior in the Cybersecurity Compendium specifies users are not to store or transport any DOT sensitive information on any portable storage media or device unless it is encrypted using DOT-approved encryption.

We were not able to validate whether backup media was encrypted for the MARAD system tested due to lack of evidence provided.

Monitoring of Unauthorized Mobile Devices

NIST SP 800-53, AC-19, Access Control for Mobile Devices, requires organizations to monitor for unauthorized connections of mobile devices to organizational information systems. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Systems which provide network access to portable and mobile devices must implement a means to detect unauthorized devices and block their access to DOT networks and systems.

DOT policy requires monitoring for unauthorized connections of mobile devices to DOT information systems. Systems which provide network access to portable and mobile devices must implement a means to detect unauthorized devices and block their access to DOT networks and systems. We noted that the DOT Cyber Security Management Center (CSMC) employs Tivoli Endpoint Manager BigFix to scan the network for unauthorized devices; however, follow-up action of unauthorized devices was not provided.

According to the Cybersecurity Compendium, the Chief Information Officer (CIO) is responsible for developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements. Operating Administration CIOs typically oversee personnel with significant responsibilities for information security and ensure that personnel are adequately trained. The DOT CIO did not ensure adequate oversight of OA cybersecurity programs to ensure technology controls are implemented and operating according to federal requirements and DOT policy in order to assist with safeguarding the confidentiality of PII. Additionally, the OA Privacy Officers did not ensure specific privacy related security controls for their systems were in effect to ensure systems were compliant with DOT password configuration requirements, backup media was encrypted, remote access controls were fully implemented including two-factor authentication and a time-out function for remote access, and monitoring of unauthorized mobile devices to include follow-up action for unauthorized devices.

A lack of adequate security controls may increase the risk of DOT's security as well as information integrity becoming compromised. DOT's sensitive materials, assets and PII may become subject to unauthorized access, modification, or removal.

We recommend the DOT Chief Information Officer:

Recommendation #5. 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.

We recommend the Operating Administration Privacy Officers:

Recommendation #6. 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.

Finding 5. DOT needs to improve the process of regularly reviewing privacy policy content on DOT websites

The E-Government Act and OMB guidance requires agencies to post privacy policies on agency websites used by the public on major entry points to agency's websites as well as at any web page where substantial personal information from the public is collected. In addition, according to OMB Memorandum M-00-13, *Privacy Policies and Data Collection on Federal Web Sites,* agencies must take care to ensure full adherence with stated privacy policies. The DIRMM states that individuals who provide their personal information to DOT are to be given adequate and accurate notice of the information program's data handling practices. Prior to commencing a new or modified information collection effort, all DOT elements are to include a privacy policy, or a link to a privacy policy, on the homepage and all pages that collect personal information, which is clearly labeled, easy to access, and written in plain language.

We noted that for one of 14 sampled FHWA websites, the privacy policy was not easily accessible from the home page. Upon notification of this issue to FHWA management, the Privacy Policy was made easily accessible from the home page. Additionally, 10 of 14 sampled FHWA websites contained information that was not in adherence with the stated privacy policy. The websites displayed a statement, "We do not use cookies[5] on this Web site," within the posted privacy policy. However, the websites did indeed use cookies. FHWA management indicated that the cookies were related to the DOT Google Analytics and the ForeSee Customer Satisfaction Survey and the information posted within Privacy Policy would be updated accordingly.

The FHWA Privacy Officer did not conduct a periodic review of the privacy policy posted on the FHWA websites to ensure it was accurate and accessible from major entry points. Without reviewing and accurately posting the Privacy Policy on a public website, DOT is at an increased risk that incorrect information is available to the public. The lack of transparency of the Privacy Policy can tarnish the DOT credibility along with potential legal ramifications.

[5] According to NIST SP 800-63-1, *Electronic Authentication Guideline* cookies are text files used by a browser to store information provided by a particular web site. The contents of the cookie are sent back to the web site each time the browser requests a page from the same web site. The web site uses the contents of the cookie to identify the user and prepare customized Web pages for that user, or to authorize the user for certain transactions.

We recommend the Operating Administration Privacy Officers:

Recommendation #7. Conduct an annual review their web sites ensuring proper and accurate posting of their Privacy policies.

Finding 6. DOT needs to review the current organizational structure of the privacy program to ensure effective management and accountability of the privacy policy and program

According to OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy,* each executive Department and agency ("agency") is to identify to OMB the senior official who has the overall agency-wide responsibility for information privacy issues. Consistent with the Paperwork Reduction Act, the agency's Chief Information Officer (CIO) may perform this role. Alternatively, if the CIO, for some reason, is not designated, the agency may have designated another senior official (at the Assistant Secretary or equivalent level) with agency-wide responsibility for information privacy issues. In any case, the senior agency official should have authority within the agency to consider information privacy policy issues at a national and agency-wide level.

According to the DIRMM the Chief Privacy Officer, as defined by OMB Memorandum M-05-08, is the senior official who has been identified to OMB as having overall responsibility for information privacy issues. DOT has designated the CIO for this role, responsible for the DOT Privacy Policy and Program and for providing guidance to DOT supervisors and employees concerning the implementation and application of the Privacy Act, as amended. The Departmental Privacy Officer is the individual, appointed by the CIO, who is responsible for overseeing the implementation and management of the DOT Privacy Policy and Program. The Departmental Privacy Officer is responsible for reviewing, approving and communicating DOT privacy policies, overseeing the Privacy Impact Assessment process to ensure all DOT information programs address and resolve privacy issues, renewing/revising Privacy Impact Assessments when there are changes, but not less often than every three years, reviewing, every two years, system of records notices for the Department for accuracy and ensuring amended notices are published to the Federal Register, providing guidance to OA Privacy Officers on their responsibilities and evaluating the effectiveness of DOT's compliance with the Privacy Act, as amended, to ensure the Department is in full compliance with the law and all relevant directives.

Although the DIRMM specifies that the Departmental Privacy Officer is responsible for overseeing the privacy program, including the PIA process; the current organizational structure only allows the Departmental Privacy Officer to function in an advisory role as there is not a formal line of accountability from the OA Privacy Officers to the Departmental Privacy Officer. The OA Privacy Officers report directly to the OA CIO. The Departmental Privacy Officer tracks PIA status, and reviews and adjudicates PIAs that are submitted; however within the current reporting structure, the Departmental Privacy Officer lacks the authority to be effective in overseeing the PIA process. The lack of accountability in the organizational structure of the DOT privacy program inhibits effectively administering the implementation and management of the DOT Privacy Policy and Program.

We recommend the DOT Chief Information Officer:

Recommendation #8. 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.

Finding 7. DOT needs to ensure management can demonstrate that controls are effectively implemented for safeguarding PII. In addition DOT needs to ensure management responds to notification of control weaknesses.

We noted several instances in which Operating Administration management could not demonstrate that controls were acting effectively due to lack of evidence provided. From the seven OAs selected for the audit, three of the OAs did not provide all of the documentation requested including MARAD, OST and RITA. In addition, the same OAs did not respond to our notification of findings. The lack of accountability by management affects the Departmental Privacy Officer's ability to successfully monitor the effectiveness of DOT's compliance with the Privacy Act, as amended, to ensure the Department is in full compliance with the law and all relevant directives, as the DIRMM specifies. Moreover, without management's response to notification of findings, the risk is increased that remediation of control weaknesses and improvements to the privacy program may be hindered.

SEC. 522. Of the Consolidated Appropriations Act, 2005 requires that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Moreover, FISMA requires that senior agency officials provide information security for the information and information systems that support the operations and assets under their control and periodically test and evaluate security controls and techniques to ensure that they are effectively implemented.

Furthermore, according to OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy,* agencies are required to maintain appropriate documentation regarding their compliance with information privacy laws, regulations, and policies. And, agencies have the authority to conduct periodic reviews (e.g., as part of their annual FISMA reviews) to promptly identify deficiencies, weaknesses, or risks. When compliance issues are identified, agencies are obligated to take appropriate steps to remedy them.

The DOT CIO (designated DOT Chief Privacy Officer) did not provide the necessary level of oversight and guidance to personnel responsible for the implementation of the DOT privacy program including the operating effectiveness of information security controls, to ensure the program was compliant with federal laws and regulations.

Without a robust privacy program, adequate controls may not be implemented increasing the threat of a breach of PII. This can lead to personal harm, loss of public trust, legal liability, or increased costs of responding to a breach of PII.

We recommend the DOT Chief Information Officer:

Recommendation #9. 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.

Recommendation #10. 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 notification of findings to make sure that control weaknesses are addressed.

Responses

The DOT Chief Information Officer's response to this report will be delivered directly to the DOT Assistant Inspector General for Financial and Information Technology Audits.

Appendix I – Objective, Scope, and Methodology

Objective

The objective of the audit was to evaluate DOT information management practices for the protection of PII in order to:

A. determine the accuracy of the descriptions of the use of information in identifiable form while accounting for current technologies and processing methods;
B. determine the effectiveness of privacy and data protection procedures by measuring actual practices against established procedural guidelines;
C. ensure compliance with the stated privacy and data protection policies of DOT and applicable laws and regulations; and
D. ensure that all technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in operation of the program and provide DOT with recommendations, strategies, and specific steps, to improve privacy and data protection management.

Scope

We conducted this audit 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. In assessing DOT's compliance with the requirements of Section 522, CLA evaluated the following areas:

- DOT's Privacy Policies and Procedures;
- DOT's Privacy Office;
- DOT's Privacy Monitoring and Compliance (included evaluation of PIAs and SORNs);
- Privacy vulnerability analysis of DOT's network and website; and
- Privacy Awareness and Training.

CLA performed a review of the following documentation provided by the DOT:

- DOT DIRMM, Chapter 8 Privacy Protections
- DOT Order 1351.20, U.S. Department of Transportation Rules of Conduct and Consequences Policy Relative to Safeguarding Personally Identifiable Information
- DOT Order 1351.38, DOT Privacy Policy for the Information Sharing Environment
- DOT Order 1351.37, Departmental Cybersecurity Policy
- U.S. Department of Transportation Departmental Cybersecurity Compendium
- DOT Order 1351.19, Personally Identifiable Information (PII) Breach Notification Controls
- U.S. Department of Transportation Biennial System of Records Notice (SORN) Review Process and Guidance
- Draft Departmental Privacy Risk Management Policy
- Draft Privacy Impact Assessment (PIA) Development Guide

- Draft Privacy NIST 800-53 Appendix J DOT Approach
- Privacy Office Organizational Chart
- Senior Agency Privacy Official Designation
- Senior Agency Official for Privacy (SAOP) Annual FISMA Report
- Inventory of IT Systems with Personally Identifiable Information

Methodology

1. Review of DOT's Privacy Policies and Procedures

CLA performed a thorough review of DOT's policy documentation to assess adherence to Section 522. CLA also reviewed the Senior Agency Official for Privacy (SAOP) Annual FISMA Report. In assessing the privacy policies and procedures, CLA determined compliance with federal guidelines related to privacy and protection of personal identifiable information.

2. Review of DOT's Privacy Office

CLA performed a review of DOT's Privacy Office to determine whether the office effectively and efficiently administered DOT's privacy program. In assessing the Privacy Office, CLA reviewed the agency's organization charts/structure and interviewed key privacy officials to determine whether the agency has identified roles and responsibilities for key privacy officials. CLA also interviewed the Departmental Privacy Officer to determine if she was performing all responsibilities and had sufficient resources to perform her duties. In addition, CLA determined whether the Privacy Office established processes for ensuring agency compliance with Federal and agency privacy policies. CLA also determined whether the Privacy Office implemented procedures in identifying and securing information systems containing PII.

3. Review of DOT's Privacy Monitoring and Compliance

CLA performed procedures to determine whether the Privacy Office effectively and efficiently administers DOT's privacy program. To accomplish this objective, CLA:

- Determined whether DOT identified and maintained a complete inventory of information systems containing PII and systems requiring PIAs and has conducted PIAs for the information systems.
- For a sample of seventeen information systems, CLA reviewed 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 than required or authorized uses), and how individuals can grant consent; and
    - How the information will be secured (e.g., administrative and technological controls).

- CLA performed 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), CLA reviewed procedures implemented by DOT to ensure:
    - Privacy was adequately protected and DOT management has implemented breach notification policies;
    - Procedures were in place to reduce the use of SSNs;
    - Policies existed to notify external agencies about privacy breaches; and
    - DOT has implemented policies for consequences and accountability for privacy violation.

4. **Privacy Vulnerability Analysis**

CLA 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. CLA reviewed the privacy incidents to determine whether any vulnerabilities were identified on the DOT network related to the risk of inadvertent release of information in an identifiable form from the agency's network.

In addition, CLA gained an understanding of the DOT's documented standards regarding its system's handling and tracking of PII. Once the CLA team had an understanding of the agency's policies as well as its approach to privacy compliance, the team 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. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Time-Out Function. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity;
- Log and Verify. Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required; and
- Ensure Understanding of Responsibilities. Ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities.

NIST SP 800-53 technical controls tested included:

- Access Control
    - Least Privilege – AC-6
    - Remote Access – AC-17

  - Wireless Access – AC-18
  - Access Control for Mobile Devices – AC-19
- Configuration Management
  - Configuration Settings – CM-6
- Security Assessment and Authorization
  - Information System Connections – CA-3
- Identification and Authentication
  - Identification and Authentication (Organizational Users) – IA-2
- Incident Response
  - Incident Handling – IR-4
  - Incident Monitoring – IR-5
  - Incident Reporting – IR-6
- Media Protection
  - Media Storage – MP-4
  - Media Transport – MP-5
- Planning
  - Privacy Impact Assessment – PL-5
- System and Communications Protection
  - Boundary Protection – SC-7
  - Transmission Confidentiality – SC-9

CLA 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. Our testing enabled us to determine if the information transmitting across the network boundaries is secure and identify any control weaknesses with respect to PII.

In order to conduct the website testing discussed above, CLA performed procedures for a sample of thirty-four websites to determine the following:

- Whether the website was using Secure Socket Layer (SSL) to capture and transfer Privacy Act protected user data.
- Whether the appropriate privacy policy and disclosures were posted and available for all visitors and users of the website. In addition, CLA assessed 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.
- Whether the website was in compliance with the use of tracking mechanisms.
- Whether DOT has implemented machine readability technology on its public website, such as Privacy Preferences Project Protocol (P3P).

5. Review of DOT's Privacy Awareness and Training

CLA performed procedures to determine whether the agency has established privacy training requirements in accordance with Federal and Agency guidance. In addition, CLA determined whether DOT has implemented a training program regarding role based training for individuals responsible for PII. CLA documented whether specific user roles have been identified by DOT that require role-based training.

To assist in the audit, CLA reviewed prior year reports to identify potential risk areas. The prior year reports include: *Review of DOT Privacy Policies and Procedures*, issued September 9, 2008 and the report *FISMA 2012: Ongoing Weaknesses Impede DOT's Progress Toward Effective Information Security* issued November 14, 2012. CLA also reviewed the report FISMA 2013: *DOT Has Made Progress, But Its Systems Remain Vulnerable to Significant Security Threats* issued November 22, 2013. Additionally, CLA reviewed DOT's policies, procedures and records and conducted interviews of DOT employees.

Appendix II – Summary of Key Criteria Tested

	Policy Requirement	Audit Conclusion
1	**Sec 522 of the 2005 Appropriations Act**	
1.a	Assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of information in an identifiable form	Issue Noted. See Recommendation #6 and 7.
1.b	Assuring that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program	Issue Noted. See Recommendation #10.
1.c	Assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act of 1974	No issues noted.
1.d	Evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the federal government	No issues noted.
1.e	Conducting a privacy impact assessment of proposed rules of the department on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected	No issues noted.
1.f	Preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementations of section 552a of title 5, 11 United States Code, internal controls and other relevant matters	No issues noted.
1.g	Ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction	Issue Noted. See Recommendation #6 and 7.

	Policy Requirement	Audit Conclusion
1.h	Training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies	No issues noted.
1.i	Each agency shall prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency	No issues noted.
1.j	Each agency shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. Such procedures shall be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002.	Issue Noted. See Recommendation #1.
2	**Privacy Act of 1974**	
2a	Agencies are to report to OMB a brief summary of changes to the total inventory of personal data systems subject to the provisions or the Act including reasons for major changes	Issue Noted. See Recommendation #4 and 5.
2.b	Publication of SORNs	Issue Noted. See Recommendation # 2 and 3.
2.c	Identify each system of records which the agency maintains	No issues noted.
2.d	Establish reasonable administrative, technical and physical safeguards to assure that records are disclosed only to those who are authorized to have access	Issue Noted. See Recommendation #6 and 7.

	Policy Requirement	Audit Conclusion
3	**E-Government Act of 2002**	
3.a	Agencies are to (1) conduct Privacy Impact Assessments (PIA) of information technology and collections and, in general, make PIAs publicly available; (2) post privacy policies on agency Web sites used by the public; and (3) translate privacy policies into a machine-readable format.	Issue Noted. See Recommendation # 2 and 3.
4	**OMB M-07-16**	
4.a	Review and Reduce the volume of PII	No issues noted.
4.b	Reduce the Use of Social Security Numbers	Issue Noted. See Recommendation # 2 and 3.
4.c	Encrypt 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.	Issue Noted. See Recommendation #6 and 7.
4.d	Allow remote access only with two factor authentication where one of the factors is provided by a device separate from the computer gaining access	Issue Noted. See Recommendation #6 and 7.
4.e	Use a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity	Issue Noted. See Recommendation #6 and 7.
4.f	Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required	No issues noted.
4.g	Implement procedures for detecting, reporting and responding to security incidents	No issues noted.
4.h	Rules and consequences policy	No issues noted.

	Policy Requirement	Audit Conclusion
5	**OMB M-03-22**	
5.a	Conduct PIAs for electronic information systems and collections and, in general, make them publicly available	Issue Noted. See Recommendation # 2 and 3.
5.b	Post privacy policies on agency websites used by the public	Issue Noted. See Recommendation #8.
5.c	Translate privacy policies into a standard machine-readable format	No Issues noted.
5.d	Report annually to OMB on compliance with section 208 of the E-Government Act	No issues noted.
6	**OMB M-05-08**	
6.a	Agencies are required to maintain appropriate documentation regarding their compliance with information privacy laws, regulations, and policies. And, agencies have the authority to conduct periodic reviews (e.g., as part of their annual FISMA reviews) to promptly identify deficiencies, weaknesses, or risks. When compliance issues are identified, agencies are obligated to take appropriate steps to remedy them.	Issue Noted. See Recommendations #9 and 10.
6.b	Each executive Department and agency ("agency") is to identify to OMB the senior official who has the overall agency-wide responsibility for information privacy issues. Consistent with the Paperwork Reduction Act, the agency's Chief Information Officer (CIO) may perform this role.	No issues noted.
7	**OMB M-06-19**	
7.a	Report security incidents to a Federal incident response center (US-CERT) within one hour of discovering the incident.	No issues noted.
8	**OMB M-10-22**	
8.a	Federal agency use of web measurement and customization technologies	No issues noted.

	Policy Requirement	Audit Conclusion
9	**OMB M-00-13**	
9.a	Ensure full adherence with stated privacy policies	Issue Noted. See Recommendation #8.
10	**OMB M-99-18**	
10.a	Posting of privacy policies on major entry points to agency's websites as well as at any web page where substantial personal information from the public is collected	Issue Noted. See Recommendation #8.
11	**NIST SP 800-122**	
11.a	Awareness, Training, and Education	No issues noted.
11.b	Security Controls	Issue Noted. See Recommendation #6 and 7.