REVIEW OF DOT PRIVACY POLICIES AND PROCEDURES

Department of Transportation

Report Number: FI-2008-077
Date Issued: September 9, 2008

Memorandum

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

Subject: ACTION: Review of DOT Privacy Policies and Procedures
Report Number FI-2008-077

Date: September 9, 2008

From: Rebecca C. Leng
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: Daniel G. Mintz
Chief Information and Privacy Officer, DOT

This report summarizes the results of our audit of the Department of Transportation's (DOT) protection of privacy information. DOT has determined that more than 100 of its 429 computer systems contain personally identifiable information (PII) about the public and DOT employees. Twelve of the 13 Operating Administrations in DOT, including the Office of Inspector General (OIG), contain 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 the PII that it collects and uses. The Act required agencies to create a Chief Privacy Officer position, submit a benchmark report on the privacy program to Congress and the Inspector General, and have an independent audit of the privacy program performed.

We contracted with an independent firm to perform the audit, as required by law. In addition to this contract audit, OIG has conducted other privacy-related audits[2]

[1] Public Law 108-447.

[2] *Audit of Security and Controls Over the National Driver Register*, OIG Report Number FI-2008-003, October 29, 2007; *DOT's Information Security Program*, OIG Report Number FI-2007-002, October 23, 2006, and OIG Report Number FI-2008-001, October 10, 2007. All of these publications can be found on our Web site at www.oig.dot.gov.

and is in the process of reviewing systems that contain PII concerning millions of commercial vehicle drivers and airmen.[3]

The objectives of this audit were to determine whether (1) the necessity of using PII for processing was properly evaluated; (2) the Department had established adequate procedures governing the collection, use, and security of PII; and (3) Operating Administrations properly complied with prescribed procedures to prevent unauthorized access to, or unintended use of, PII.

The audit was completed by Clifton Gunderson, LLP, of Calverton, Maryland, under contract to the DOT OIG, and by OIG staff in accordance with generally accepted government auditing standards as prescribed by the Comptroller General of the United States and included such tests as we considered necessary to detect fraud, waste, or abuse. We performed a quality control review of the audit work performed by Clifton Gunderson to ensure that it complied with generally accepted government auditing standards. In our opinion, Clifton Gunderson's audit work complied with applicable standards. Details of the scope and methodology can be found in Exhibit A.

FINDINGS

Clifton Gunderson concluded that DOT made significant progress in addressing its statutory responsibilities under the Act by designating a senior official—the departmental Chief Information Officer—to be the Chief Privacy Officer.[4] The Chief Information and Privacy Officer issued a privacy benchmark report to Congress and the OIG in September 2006. His office also maintains an inventory of PII systems.

Clifton Gunderson also concluded that DOT has established proper procedures and a framework for assessing the necessity of using PII and the collection, use, and security of PII. However, tests of 20 sample PII systems identified deficiencies in compliance with the prescribed procedures. (The contractor's complete report can be found in Appendix A). As shown in the table on pages 15 and 16, 15 of the 20 systems sampled had at least one control deficiency.

[3] Audit initiated on *Information Security and Privacy Controls of FAA Medical Support System*, OIG Project Number 08F3006F000, February 28, 2008; and audit initiated on *Data Integrity of the Commercial Driver's License Information System*, OIG Project Number 08F3003F000, December 5, 2007.

[4] Day-to-day oversight of DOT PII compliance operations is delegated to the privacy officers in the Chief Information Officer's office and in individual Operating Administrations.

The following summarizes the contractor's findings:

1. The DOT Privacy Office did not provide evidence to support the effectiveness of procedures used in evaluating and identifying Operating Administration systems containing PII. The departmental privacy office had evaluation documents for only the 109 systems contained in its PII inventory. The office could not provide completed evaluations to support that no PII is stored in 320 of DOT's 429 systems. DOT has no assurance that all systems containing PII have been identified for protection.

2. Deficiencies existed in DOT's collection, security protection controls, and notification of the public concerning PII system data. The contractor found that 9 of 20 sampled systems requiring a System of Records Notice (SORN) did not have one published. As a result, the public was not properly notified of the intended use of the information collected from it. In addition, 1 of 20 systems requiring a Privacy Impact Assessment (PIA) did not have one performed and 2 of 5 sampled systems that share privacy information with outside agencies did not have memoranda of understanding to ensure proper security protection of PII by the recipient agencies.

3. Twelve of the 20 sampled PII systems did not encrypt their PII data for network transmission. This is in direct noncompliance with DOT PII security policy 2006-22 for protection of PII. This can lead to unauthorized review of these data during transmission and/or exploitation of these systems for malicious intent.

4. Four of the 20 sampled PII systems did not have basic DOT password security controls, such as appropriate password length and complexity, password expiration, number of invalid log-in attempts, and session time-out expiration. Lack of compliance with these DOT security control policies could enable unauthorized users to crack passwords and obtain access to PII systems and data.

5. The departmental and Operating Administration privacy officers did not receive more privacy regulation and PII security protection training than the average departmental employee. This may have directly affected the privacy officers' ability to understand the statutory requirements necessary to identify PII systems and fully implement adequate security protection controls over their PII systems identified in this audit.

Further, the Act requires privacy officials to ensure that the use of technology does not erode protection of privacy information. However, in a matter that we view as also related to training and that was not part of the contractor's report, DOT experienced an incident during early 2007 in which one of its privacy officers

stored PII on a home computer with peer-to-peer file-sharing capabilities. As a result, an unauthorized user on the Internet was able to download this information.[5] Enhanced privacy and security training may have prevented this incident.

In conjunction with the contractor's review, OIG staff examined security protection of the Web sites developed for two sampled systems.[6] Web technologies are commonly used to allow authorized users to access information from the Internet. OIG staff identified significant deficiencies in these Web sites that could allow Internet hackers to gain unauthorized access to the PII stored in these two systems.[7] This occurred because these Web sites were not properly configured in accordance with departmental standards.

We also noted that the departmental privacy officer does not report directly to the Chief Information and Privacy Officer. The Chief Information and Privacy Officer delegated the responsibility of establishing privacy policies and managing the Department's privacy program to the departmental privacy officer. However, this key position reports to the Acting Chief Information Security Officer, who in turn reports to the Chief Information and Privacy Officer and whose primary responsibility is information security, not privacy. In our opinion, this organizational structure has reduced the visibility of the privacy program and was a major contributing factor to the deficiencies identified in this audit. Having the departmental privacy officer report directly to the Chief Information and Privacy Officer could increase management awareness and provide closer scrutiny of Operating Administrations' corrective actions.

We provided a draft report to the DOT Chief Information and Privacy Officer for comment on July 8, 2008, and on August 19th we received the response. The Chief Information and Privacy Officer concurred or concurred in part with all of our recommendations, and stated that his office is in the process of acquiring and implementing technology to ensure that no PII can be obtained from DOT systems and infrastructure by unauthorized parties. The response can be found in its entirety in Appendix B.

---

[5] Testimony of Daniel G. Mintz, Chief Information Officer, DOT, before the Committee on Oversight and Government Reform, House of Representatives, July 24, 2007.

[6] Web technologies were used in 4 of 20 sampled systems. Due to logistical limitations, we were able to examine only two systems.

[7] For security reasons, specifics concerning the weaknesses and vulnerabilities that we identified and our audit procedures are not discussed in this report but were provided to Operating Administration privacy officers.

RECOMMENDATIONS

Based on both Clifton Gunderson and OIG findings, we recommend that the departmental Chief Information and Privacy Officer:

1. Require system owners to submit evaluation results on whether PII exists in the 320 systems that were not included in the DOT Privacy Office inventory.

2. Require system owners of sampled systems to correct privacy protection deficiencies identified in the areas of missing SORNs, PIAs, and memoranda of understanding with outside agencies when sharing PII; and notify system owners of remaining PII systems to check whether they need to take similar corrective actions.

3. Require Operating Administration privacy officers to implement a process under which future systems are subject to periodic review to ensure that SORNs are initiated and posted, PIAs are developed, and memoranda of understanding with outside agencies are documented; and that such elements are appropriately updated when systems undergo change.

4. Encrypt all PII data transmitted over the Department's communications network.

5. Require system owners of sampled systems to correct security deficiencies concerning password security controls, invalid log-in attempts, and session time-out expiration; and notify system owners of remaining PII systems to check whether they need to take similar corrective actions.

6. Require Operating Administration privacy officers to implement a process under which periodic performance checks are carried out to ensure that all PII systems remain in full compliance with DOT security policies.

7. Provide enhanced privacy security training for Operating Administration privacy officers, who are responsible for implementing annual privacy practices in their respective organizations.

8. Require system owners of sampled systems to correct security deficiencies found in their Web sites; and notify system owners of remaining PII systems to check whether they need to take similar corrective actions.

9. Increase the visibility of the DOT Privacy Program by having the departmental privacy officer report directly to the Chief Information and Privacy Officer.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided a draft report to the DOT Chief Information and Privacy Officer for comment on July 8, 2008, and on August 19th we received the response. The Chief Information and Privacy Officer concurred or concurred in part with all of our recommendations, and stated that his office is in the process of acquiring and implementing technology to ensure that no PII can be obtained from DOT systems and infrastructure by unauthorized parties. The response can be found in its entirety in Appendix B.

In general, management actions—begun and planned—adequately address the intent of our recommendations, with the exception of recommendations 1 and 4. The responses to our recommendations are summarized as follows:

Recommendation 1: The Chief Information and Privacy Officer concurred. In the response, it was stated that the results of an August 2007 survey of all DOT systems to determine which contained PII are now available for Office of Inspector General review—including those not previously made available. However, our review of the new information provided by management still found no support that PII was not contained in the 320 systems questioned in our report. Therefore, as originally recommended, the Chief Information and Privacy Officer should require system owners to submit evaluation results to ensure that PII does not exist in these 320 systems.

While not part of our recommendation, the Privacy Office has proposed that a Privacy Threshold Analysis be performed during initial system certification and accreditation and reaccreditation to determine whether the system contains PII. The Office of the Chief Information and Privacy Officer has set a target date of March 31, 2009, for implementation. We support this planned action.

Recommendation 2: The Chief Information and Privacy Officer concurred. System owners responsible for missing or outdated Privacy Impact Assessments and Systems of Records Notices have been notified for correction, and owners of systems containing PII will be notified, by March 31, 2009, to address and update memoranda of understanding with outside agencies.

Recommendation 3: The Chief Information and Privacy Officer concurred. The recommended actions—requiring Operating Administration privacy officers to implement a process under which future systems are subject to periodic review for initiation and posting of Systems of Records Notices, development of Privacy Impact Assessments, and documentation of memoranda of understanding with outside agencies—coincide with DOT's privacy policy and will be implemented

through appropriate direction to Operating Administration CIOs and privacy officers, and in DOT/CIO policy by March 31, 2009.

Recommendation 4: The Chief Information and Privacy Officer concurred. His office is presently conducting a detailed analysis of system and encryption requirements and anticipates that this analysis will be completed by March 31, 2009. Based on the analysis, a detailed action plan will then be developed to implement encryption requirements.

While the Chief Information and Privacy Officer provided us with a plan of action and date of completion for the analysis of encryption requirements, no date was provided for the completion of actually encrypting the transmission of PII over the Department's network. The Chief Information and Privacy Officer should provide a target date for completing this action, which has been a departmental requirement since 2006.

Recommendation 5: The Chief Information and Privacy Officer concurred. He anticipates that systems containing PII can be secured by July 31, 2009. In addition, his office will address issues identified in the report with Operating Administration CIOs, information system security officers, privacy officers, system owners, and other responsible parties**.**

Recommendation 6: The Chief Information and Privacy Officer concurred. His office will issue a directive by December 31, 2008 for Operating Administration privacy officers to conduct performance checks to ensure that they remain in full compliance with DOT security policies. A final policy memorandum, incorporating feedback from the directive, will be issued by March 31, 2009.

Recommendation 7: The Chief Information and Privacy Officer concurred. By written notification to modal privacy officers, he will require the owners of sampled systems to correct security deficiencies on their Web sites. He will also direct modal privacy officers, CIOs, and information system security officers to work with owners of all systems containing PII to identify any necessary corrective actions and develop corrective action plans by March 31, 2009.

Recommendation 8: The Chief Information and Privacy Officer concurred. He has recommended specialized training for Operating Administration privacy officers, and his office will establish such requirements—both for content and frequency—by March 31, 2009.

Recommendation 9: The Chief Information and Privacy Officer partially concurred. He cited a tradeoff between increasing the visibility of the DOT Privacy Program by having the departmental privacy officer report directly to the

Chief Information and Privacy Officer versus keeping the current reporting relationship. While acknowledging that increased visibility for the Privacy Office would be beneficial, he cited the "synergies" and "more efficient use of staff collectively" as reasons for favoring the current structure. He further stated that perhaps some of the issues identified in our report resulted from personnel changes occurring at the time of our review and, therefore, that such a reporting shift might not accomplish much.

Therefore, the Chief Information and Privacy Officer favored leaving the current structure as is for the next fiscal year—focusing on implementing suggested changes, enhancing associated internal auditing reviews, and developing more transparent measures of operating status—then reexamining whether changing the reporting structure is needed at the end of Fiscal Year 2009. This planned action meets the intent of our recommendation. We plan to follow up on this issue through next year's review of the Department's information security program.

ACTIONS REQUIRED

Except for recommendations 1 and 4, the actions begun and planned by the Chief Information and Privacy Officer are responsive to our recommendations and are considered resolved subject to follow-up requirements in DOT Order 8000.1C. We would appreciate receiving the Chief Information and Privacy Officer's updated response to include revised completion dates for recommendations 1 and 4 within 30 days.

We appreciate the courtesies and cooperation of the DOT Office of the Chief Information and Privacy Officer, DOT Operating Administration privacy officers, and Clifton Gunderson representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407 or Nathan Custer, Program Director, at (202) 366-5540.

#

cc: General Counsel
DOT Chief Information Officer's Council Members
Martin Gertel, M-1

EXHIBIT A. SCOPE AND METHODOLOGY

This audit was conducted by Clifton Gunderson, LLP, of Calverton, Maryland, under contract to DOT OIG, and by OIG staff. The audit was conducted at selected DOT Operating Administrations in Washington, D.C. and field sites. The following summarizes the contractor's scope and methodology:

- The contractor reviewed DOT's benchmark report to the OIG prepared in fulfillment of Section 522-c of the Appropriations Act and dated September 26, 2006.

- The contractor reviewed and analyzed privacy policies, guidance, and reports, and interviewed officials from the Privacy Office.

- The contractor analyzed the System of Records Notice and Privacy Impact Assessment development processes and assessed the progress of the office in implementing these processes.

- The contractor selected a representative sample of 20 systems for testing of security controls, publication of System of Records Notice, and performance of the Privacy Impact Assessment.

Details can be found on pages 18, 19, and 20 of Appendix A of this report.

The OIG staff examined security protection of Web sites developed for two sampled systems. We did this by examining policies and procedures, observing controls in operation, and using a commercial tool to assess the vulnerability of the Web sites.

The audit work was performed between December 2007 and May 2008. This performance audit was conducted in accordance with generally accepted government auditing standards prescribed by the Comptroller General of the United States and included such tests as we considered necessary to detect fraud, waste, and abuse.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Nathan Custer	Program Director
Dr. Ping Sun	Program Director for IT Audit Computer Laboratory
James Mallow	Contracting Officer's Technical Representative
Michael P. Fruitman	Communications Adviser
Vasily Gerasimov	Information Technology Specialist

APPENDIX A. REPORT ON THE 2007 REVIEW OF DOT's COMPLIANCE WITH SECTION 522 OF THE CONSOLIDATED APPROPRIATIONS ACT OF 2005

UNITED STATES DEPARTMENT OF TRANSPORTATION (US-DOT)

Report on the 2007 Review of DOT's Compliance with Section 522 of the Consolidated Appropriations Act, 2005.

(Policies, Procedures & Practices for Protection of Personally Identifiable Information)

Clifton Gunderson LLP

February 29, 2008

Clifton Gunderson LLP
Certified Public Accountants & Consultants

Ms. Rebecca C. Leng
Assistant Inspector General for Financial and
Information Technology Audits
Office of the Inspector General
U.S. Department of Transportation
1200 New Jersey Avenue SE
Washington, DC 20590

Dear Ms. Leng

We are pleased to present our report on the Department of Transportation's (DOT) compliance with protection of personal data in an identifiable form. This review included assessing compliance with applicable federal security and privacy laws and regulations as well as assessing the privacy and data protection procedures used by DOT as they relate to the guidelines set forth in Section 522-d of the *Omnibus Spending Bill for Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005*. The objective of our review was to determine whether: (1) the necessity of using personally identifiable information for processing was properly evaluated; (2) the Department had established adequate procedures governing the collection, use and security of personally identifiable information; and (3) Operating Administrations (OAs) properly complied with the prescribed procedures to prevent unauthorized access to and unintended use of personally identifiable information.

We interviewed key personnel involved in identifying and protecting personally identifiable information and reviewed documentation supporting DOT's efforts to comply with federal privacy and security laws and regulations.

This performance evaluation was conducted from October 2007 to January 31, 2008 at the DOT headquarters in Washington, DC and was conducted in accordance with *Generally Accepted Government Auditing Standards*.

We appreciate the opportunity to have served you once more and are grateful for the courtesy and hospitality extended to us by DOT personnel. Please do not hesitate to call me at (301) 931-2050 or email at george.fallon@cliftoncpa.com if you have questions.

Sincerely,

CLIFTON GUNDERSON LLP

Clifton Gunderson LLP

Calverton, Maryland
February 29, 2008

11710 Beltsville Drive
Suite 300
Calverton, Maryland 20705
tel: 301-931-2050
fax: 301-931-1710
www.cliftoncpa.com

Appendix A. Report on the 2007 Review of DOT's Compliance With Section 522 of the Consolidated Appropriations Act of 2005

EXECUTIVE SUMMARY

The DOT Office of the Chief Information Officer (OCIO) Privacy Office has been proactive in carrying out its statutory responsibilities and its related role in ensuring compliance with Section 522 of the General Government Appropriations Act of 2005. Specifically, the Privacy Office has established a framework for identifying information systems containing or processing personally identifiable information (PII), securing data contained in these systems, conducting Privacy Impact Assessments (PIA) and reporting Systems of Records Notices (SORNs), all required by the Act. The Office of the Secretary of Transportation performs cyclical checks to ensure OA's comply with these requirements and maintains a weekly scorecard of these activities.

Based on our review, DOT has (a) evaluated the necessity of using PII for data processing; (b) established procedures for the collection, use and security of PII and (c) Operating Administrations complied with the prescribed procedures to prevent unauthorized access to and unintended use of PII. However more work remains to be accomplished. Specifically, we noted the following:

Although the DOT OCIO and Privacy Office have established policies and procedures to protect DOT's PII systems and data, the Privacy Office does not properly monitor its privacy processes for quality compliance with the provisions of Section 522.

- DOT did not provide evidence to support the effectiveness of the procedures used in identifying and securing information systems containing PII. The Privacy Office could not provide evidence that evaluations were performed for all four hundreds and twenty-nine DOT systems that may potentially contain and/or process PII.
- DOT did not provide evidence that the Privacy Office had a structured format to monitor the effectiveness and completeness of PIAs and SORNs implemented by the different OAs on affected systems. (DOT did not have a permanent Departmental Privacy Officer during our review period from October 2007 through January 2008). Limited resources and/or personnel could account for this lack of adequate monitoring resulting in the following:
  - A Privacy Impact Assessment (PIA) had not been performed for one (1) out of twenty (20) systems in our sample. This system contained public PII and required a PIA.
  - SORNs were not published for nine (9) out of twenty (20) sample systems tested. While the Privacy Office has reviewed, approved, and issued new SORNs since its establishment, we identified nine sampled systems did not have SORN notices published. The department is not in compliance with the Office of Management and Budget (OMB) requirements that SORNs be published and reviewed semi-annually, nor can it be assured that the privacy implications of its many systems that process and maintain PII have been fully and accurately disclosed to the public. These notices should identify, among other things, the type of data collected, the types of individuals about whom information is collected, and the intended uses of the data.
- DOT OAs had not established Memoranda of Understandings (MOU) for two (2) out of five (5) systems from our sample of twenty systems that share privacy data with external agencies. Also, the PIAs reviewed did not provide guidance on privacy

information sharing with other agencies. These PIAs did not include measures to escalate requests from federal agencies (law enforcement bureaus) that may require PII for legitimate government business.

- DOT Privacy Office had not provided enhanced privacy security training to OA Privacy Officers as well as their representatives who are responsible for deploying DOT's PII policies at their respective OAs. DOT does provide its employees with security awareness training. Per the responses on the OCIO FISMA template for September 2007, eighty-six percent of DOT employees have received security training for fiscal year 2007. Although security protection of PII data was part of these training courses, the agency's Privacy Officers did not receive enhanced privacy security training to assist them in understanding all integral parts of their job responsibilities.

DOT technical controls related to the protection of personally identifiable information need to be strengthened.

- Twelve (12) out of twenty (20) sampled PII systems reviewed do not encrypt their PII data and transmit this data over DOT's network in clear unencrypted text.
- Four (4) out of twenty (20) systems were non-compliant with DOT security policies concerning basic password security requirements, specifically: (1) number of login attempts on two systems in our sample (10%) was set to expire after six unsuccessful logon attempts; (2) password parameters for one system requires the password to be changed every 180 days contrary to DOT policy of 90 days; (3) One system had not implemented secure password settings such as password complexity, number of invalid login attempts, session expiration and password expiration.

DOT consists of the Office of the Secretary and eleven individual 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 Saint Lawrence Seaway Development Corporation, the Research and Special Programs Administration, the Bureau of Transportation Statistics, and the Surface Transportation Board.

The following table summarizes the sample of systems reviewed and exceptions noted:

#	OA	System Description	Results of Tests		
			Systems of Records Notices	Privacy Impact Assessments	Technical Controls
1	FAA	Delphi tracking System (DTF)	SORN not published		
2	FAA	Enforcement Information System (EIS)	SORN not published	PIA required but not yet developed	No data encryption.
3	FAA	MedXPress			Password settings not consistent with DOT policy. No data encryption.
4	FAA	Safety Performance Analysis System (SPAS)	SORN not published		Password settings not consistent with DOT policy. No data encryption.
5	FAA	Airman Registry Modernization System (RMS)			No data encryption.
6	FHWA	User Profile Access Control System (UPACS)			
7	FHWA	National Highway Institute (NHI)			Password settings not consistent with DOT policy.
8	FMCSA	Electronic Document Management System (EDMS)	SORN not published		
9	FMCSA	Medical Exemption System (MEDEX)	SORN not published		No data encryption.
10	FRA	Correspondence Control & Management System (CCM)	SORN not published		Password settings not consistent with DOT policy. No data encryption.
11	FTA	DOTS/DOT2000 Financial Management System	SORN not published		No data encryption.
12	MARAD	MSCS			
13	MARAD	Personnel Management Information System (PMIS)			
14	NHTSA	Motor Vehicle Importation Information System (MVII)			No data encryption.
15	OIG	Transportation Inspector General Reporting System (TIGR)			No data encryption.

#	OA	System Description	Results of Tests		
			Systems of Records Notices	Privacy Impact Assessments	Technical Controls
16	OST	Security Operations System	SORN not published		No data encryption.
17	OST	Investigative Tracking System			
18	PHMSA	HMIS			
19	RITA	Volpe ADP Institutional Support Services (RITAX0013)	SORN not published		No data encryption.
20	STB	Case Management System			No data encryption.

BACKGROUND

The Privacy Act of 1974 requires agencies to "establish appropriate administrative, technical and physical safeguards to ensure 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 the information is maintained," 5 U.S.C. § 552a (e) (10). The Privacy Act limits agencies to "maintaining 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," 5 U.S.C. § 552a (e) (1).

The E-Government Act of 2002 strives to enhance protection of personal information in government information systems, by requiring the agencies to conduct PIAs. A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system.

Today's DOT Privacy Program consists of a partnership between the Office of the Chief Information Officer (OClO)/Privacy Office and the Office of the General Counsel (OGC). Additionally, the program collaborates with DOT's Information Assurance Office/OCIO/OST on those issues that incorporate both privacy and security, focusing frequently on the security of technology that may adversely affect the privacy of individuals.

Section 522 of the 2005 Consolidated Appropriations Act for Transportation and Treasury, Public Law 108-447, Division H, provides additional privacy requirements for DOT, including the implementation of privacy policies and procedures for public and employee data. The legislation also requires DOT to designate a Chief Privacy Officer. OMB Memorandum-05-08 also requires each department to designate a Senior Agency Official for Privacy. For DOT, the Chief Information Officer also serves as the Senior Agency Official for Privacy.

Section 522(c) of the above-mentioned Act further requires that DOT:

> "...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. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report. By signing the report, the privacy officer also verifies that the agency is only using information in identifiable form as detailed in the report. "

DOT's use of personally identifiable information and related policies and procedures

DOT collects and uses a significant amount of personally identifiable information of both employees and the public. The DOT Privacy Program is administrated within DOT's OCIO and OGC, both located in the Office of the Secretary of Transportation (OST).

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 (OMB) privacy guidance.

The DOT Privacy Program has an on-going initiative to grow the skills, knowledge and capabilities of the privacy officers of all OAs (who are on the front line of the DOT's efforts to enhance privacy protection).

In conformity with the 2005 Consolidated Appropriations Act, the DOT's Office of the Chief Information Officer published a Privacy Benchmark report in September 2006. This report was sent to the DOT OIG and to Congress. This report outlines the following areas:

- *DOT Privacy Program:* Includes an overview of DOT's privacy management program established in 2003 and Section 522 benchmark-reporting requirement.
- *DOT Use of PII, Privacy and Data Protection Policies and Procedures:* Includes an overview of efforts used to track PII, DOT privacy officer's compliance efforts, DOT-wide policies and procedures developed or drafted to date in compliance with various privacy laws, regulations and OMB guidance, and other key privacy initiatives.
- *OA Use of PII and Privacy Practices:* Includes reports on each OA's specific PII and privacy program activities.

DOT's mission is to ensure a safe and efficient national transportation system. In doing so, DOT is required to collect and use a significant amount of personal information from employees and the public for both administrative and operational initiatives. To ensure information collected is secure, DOT has appointed a departmental privacy officer located within the OCIO, as well as privacy officers within each OA. In addition to providing leadership on DOT-wide policies and procedures, the DOT Privacy Program works collaboratively with each OA's privacy officer to guide and support their privacy awareness and compliance efforts. The methodology is based upon the following:

- Establish the priority, authority, and responsibility,
- Assess current privacy environment,
- Organize resources necessary for the project's goals,
- Develop policies, procedures and practices,
- Implement policies, practices and procedures,
- Maintain the policies, practices and procedures,
- Manage the exceptions and/or problems with the policies, practices and procedures.

In compliance with this requirement, DOT undertook a review of the use of PII and privacy policies and procedures at both the DOT-wide and OA levels. In preparing the ensuing privacy benchmark report, the DOT Privacy Officer obtained input from each OA Privacy Officer on their specific privacy activities.

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 109 such systems. The FAA, FMCSA, and FHWA maintain the largest number of PII systems.

Given the significant amount of sensitive PII data handled by the DOT, the DOT Privacy Officer continually works to track PII use and identify weaknesses that may require corrective action at the program or system level. A critical part of this process involves the review of PIAs and SORNs (if applicable) that are prepared by each PII system owner. In some cases, however, a PII system may be exempt from the requirement to perform a PIA if this system was created or implemented prior to the enactment of the E-Government Act of 2002. The DOT Privacy Office maintains a list of all PII systems that have completed a PIA or SORN and is responsible for posting all final PIAs and SORNs on the DOT Privacy Program web page.

SCOPE AND METHODOLOGY

DOT's OIG contracted with Clifton Gunderson LLP to conduct an audit of DOT's privacy and data protection policies and procedures in compliance with Section 522. The objective of this review was to assess the progress of DOT's Privacy Office in carrying out its responsibilities under federal law, more specifically, to determine whether: (1) the necessity of using personally identifiable information for processing was properly evaluated; (2) DOT had established adequate procedures governing the collection, use and security of personally identifiable information; and (3) Operating Administrations (OAs) properly complied with the prescribed procedures to prevent unauthorized access to and unintended use of personally identifiable information.

To address this objective, we reviewed federal statutes including the Privacy Act of 1974 and Section 208 of the E-Government Act, to identify responsibilities of DOT's Privacy Office. We reviewed and analyzed privacy policies, guidance, and reports, and interviewed with officials from the Privacy Office. The personnel interviewed included the Chief Privacy Officer (CPO) to identify privacy office's plans, priorities, and processes for implementing its responsibilities using available resources.

We further evaluated the Privacy Office policies, guidance, and processes for ensuring compliance with the Privacy Act, and the E-Government Act. We analyzed the SORNs and PIA development processes and assessed the progress of the office in implementing these processes. This analysis included analyzing the Privacy Office's overview of PIAs developed by each OA and assessing the overall quality of published PIAs.

Perform an assessment of DOT's privacy policies

We reviewed DOT information management practices for protection of PII, as they relate to the guidelines set forth in Section 522-d of the 2005 Government Appropriations Act. Public Law 107-347, the E-Government Act of 2002, defines "identifiable form" as *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.* We performed procedures to assist the OIG in evaluating DOT's information management practices 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.
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.
E. Provide DOT with recommendations, strategies, and specific steps, to improve privacy and data protection management.

We examined DOT's PII policies, practices and data protection procedures and mechanisms in operation. Specifically, the tasks focused on:

- Reviewing DOT's technology, practices and procedures with regard to the collection, use, sharing, disclosure, transfer and storage of information in identifiable form.
- Reviewing DOT'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 DOT's employees and the public.

The E-Government Act of 2002 requires agencies to conduct a PIA either (1) before developing or procuring information technology systems or projects that collect, maintain or disseminate information in identifiable form or (2) when initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government). In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks, for example, when converting paper-based records to electronic systems. On the other hand, no PIA is required where (1) information relates to internal government operations, (2) has been previously assessed under an evaluation similar to a PIA, or (3) where privacy issues are unchanged.

To accomplish the above-mentioned objectives, we:

- Reviewed DOT's benchmark report to the OIG dated September 26, 2006. This report was prepared in fulfillment of Section 522-c of the Appropriations Act. "…*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. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report. By signing the report, the privacy officer also verifies that the agency is only using information in identifiable form as detailed in the report."*
- Reviewed DOT's policies related to safeguarding PII; encryption of sensitive PII and guidelines for the protection of remote PII through secure remote access (SRA). [Policy # 2006-22 Revision 1] of October 11, 2006.
- Verified that DOT had identified and maintained an inventory of information systems containing PII and systems requiring PIAs and had conducted PIAs for electronic information systems.
- Reviewed a sample of PIAs for the following:
  - What information was collected (e.g., nature and source).
  - Why the information was collected (e.g., to determine eligibility).
  - Intended use of the information (e.g., to verify existing data).
  - With whom the information was shared (e.g., another agency for a specified programmatic purpose).
  - What opportunities individuals had to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), and how individuals communicated consent.
  - How the information was secured from abusive use (e.g., administrative and technological controls).
- We selected a representative sample of systems from OST and 10 OAs, and tested technical controls to achieve the PII protection objectives.
- Reviewed the nature and use of PII, to determine whether a SORN was required and if required, whether one was published. We further reviewed DOT's publication of SORNs in the Federal Register and verified that they contained only information about individuals that was "*relevant and necessary*" to accomplish DOT's purpose. We verified that this information was updated as necessary.

For the Fiscal Year 2007 Privacy Assessment, we were not engaged to and did not perform procedures to determine if the inventory of systems containing PII data was exhaustive and if DOT had performed procedures to ensure all 429 DOT IT systems within all OAs had been reviewed for existence of PII information. We reviewed the inventory of 109 PII systems received from the DOT OCIO privacy office in October 2007. From this population, we selected a representative sample of 20 systems from OST and 10 OAs for substantive testing. The results and exceptions noted in this report are based on this sample.

DETAILED RESULTS OF REVIEW

1. Although the DOT OCIO and Privacy Office have established policies and procedures to protect DOT's PII systems and data, the Privacy Office does not properly monitor its privacy processes for quality compliance with the provisions of Section 522.

The DOT Privacy Office has made significant progress in addressing its statutory responsibilities under the General Government Act by developing processes to ensure implementation of privacy protections in departmental programs. For example, the Privacy Office has established processes for ensuring departmental compliance with the PIA requirement in the E-Government Act of 2002. Instituting this framework has led to increased attention to privacy requirements on the part of departmental components, contributing to an increase in the number of PIAs issued.

OCIO has addressed its mandate to assure that technologies sustain, and do not erode, privacy protections through a variety of actions, including implementing a weekly scorecard of PII compliance, its PIA compliance framework, raising awareness of privacy issues through a series of workshops, and participating in policy development for several major DOT initiatives. The office has also taken action to address its mandate to evaluate regulatory and legislative proposals involving the use of personal information by the federal government and has coordinated with the DOT Office of General Counsel.

While substantial progress has been made in these areas, more work needs to be done in other important aspects of DOT's privacy protection processes. The details of the matter are as follows:

General conditions found during the audit

- DOT did not provide evidence to support the effectiveness of the procedures used in identifying and securing information systems containing PII. The Privacy Office could not provide evidence that evaluations were performed for all 429 DOT systems that may potentially contain and/or process PII.
- DOT Privacy Office had not provided enhanced privacy training to OA Privacy Officers (or their representatives), who are responsible for deploying DOT's PII policies at their respective OAs. DOT does provide its employees with security awareness training. Per the responses on the OCIO FISMA template for September 2007, only 86% of DOT employees have received security training for fiscal year 2007. Although security protection of PII data was part of these training courses, the agency's Privacy Officers did not receive enhanced privacy security training to assist them in understanding all integral parts of their job responsibilities.

Detailed conditions based on our sample of 20 DOT PII systems

- DOT did not provide evidence that the Privacy Office had a structured format to monitor the effectiveness and completeness of PIAs and SORNs implemented by the different OAs on affected systems. (DOT did not have a permanent Departmental Privacy Officer during our review period from October 2007 through January 2008). Limited resources and/or personnel could account for this lack of adequate monitoring resulting in the following:
  - A PIA had not been performed for 1 of 20 systems in our sample. This system contained public PII and required a PIA.
  - SORNs were not published for 9 of 20 sample systems tested. While the Privacy Office has reviewed, approved, and issued new SORNs since its establishment in 2003, nine sampled systems did not have these notices published. The department is not in compliance with the Office of Management and Budget (OMB) requirements that SORNs be published and reviewed biennially, nor can it be assured that the privacy implications of its many systems that process and maintain PII have been fully and accurately disclosed to the public. These notices should identify, among other things, the type of data collected, the types of individuals about whom information is collected, and the intended uses of the data.
- DOT OAs had not established MOUs for 2 of 5 systems from our sample of 20 systems that share privacy data with external agencies. Also, the PIAs reviewed did not provide guidance on privacy information sharing with other agencies. These PIAs did not include measures to escalate requests from federal agencies (law enforcement bureaus) that may require PII for legitimate government business.

Section 522 **describes Chief Privacy Officer's security responsibilities as follows:**
"…A: PRIVACY OFFICER: Each agency shall have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, including:

1. *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.*
2. *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.*

Recommendations:

We recommend that DOT:

- Implement a process for the timely review and monitoring of the privacy process to include: inventory of all affected systems; review and approval of PIAs; review and approval of SORNs prior to publication; and periodical updates of both the PIAs and the SORNs.
- Establish MOUs with all third parties who share PII with DOT.
- Implement procedures to ensure all 429 DOT systems are evaluated for existence and/or processing of PII. The DOT Privacy Office inventory identified 109 PII systems out of DOT's 429 systems. This evaluation should be documented and should cover the remaining 320 of 429 DOT information systems
- Require enhanced privacy security training for Privacy Officers at the different OAs who are responsible for implementing privacy practices at their respective OAs.

2. DOT Technical Controls related to the protection of personally identifiable information need to be strengthened.

The DOT Privacy Office has made significant effort in carrying out its statutory responsibilities and its related role in ensuring compliance with Section 522 of the General Government Appropriations Act, notably by establishing a framework for securing data contained in privacy systems. However, our review of a sample of 20 privacy systems highlighted that technical control over access to these systems needed to be strengthened. The details are as follows:

- Twelve out of 20 sampled PII systems reviewed transmit PII data over DOT's network in clear unencrypted text. Some of these systems contained public data.
- Four out of 20 systems were non-compliant with DOT security policies concerning basic password security requirements. (1) number of login attempts on two systems on our sample (10%) was set to expire after six unsuccessful logon attempts; (2) password parameters for one system requires the password to be changed every 180 days contrary to DOT policy of 90 days; (3) One system had not implemented secure password settings such as password complexity, number of invalid login attempts, session expiration and password expiration.

Department of Transportation - Information Technology and Information Assurance Policy (2006-22): **states:**

"…It is the policy of the DOT that all DOT personnel and contractors comply with the provisions of this policy. DOT will begin to implement the following provisions during the fourth quarter of Fiscal Year 2006 for any information technology system that stores, processes and/or transmits PII.

1. Encrypt all PII wherever it may reside within six months of the issuance of this policy. The encryption methodology employed shall satisfy the requirements set forth in the current National Institute of Standards and Technology Federal Information Processing Standard 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

a. Encrypt all data on mobile devices within six months of the issuance of this policy.
b. Encryption policies apply to all storage media devices, to include CDs, DVDs, disk drives, USB memory drives, SD cards, etc.

Employee Awareness Guide to Information Assurance and Technology Security (March 2006): **states:**
"…Passwords are effective only when properly used. Password and/or PIN protected screen savers should be used on all systems and set to activate after 15 minutes of non-use. Passwords, at a minimum, must be protected as sensitive information. Passwords should never be written down.

Mandatory Password Changes:
Passwords are required to be changed as indicated below:

- Every 90 days for general users.
- Every 30 days for systems administrators.
- Immediately upon completion of an investigation of a known or suspected compromise.
- The password and associated user account must be suspended within one day if the user's access is removed for reasons of pending or current punitive actions.
- When the user leaves the organization or no longer requires access for a period greater than three months, the password must be changed as soon as possible, but no later than three days.
- After three invalid login attempts, the password and login ID should be suspended…"

Recommendations:

We recommend that DOT:

- Implement encryption of data transmitted over the agency's communication infrastructure with emphasis on encryption of systems containing privacy data.
- Upgrade all systems containing sensitive personally identifiable information that are unable to support secure computing practices. Alternatively, privacy data contained in these systems should be removed or transferred to more secure platforms.
- Periodically review the agency's information systems to ensure they are in compliance with DOT IT security policies.

APPENDIX B. MANAGEMENT COMMENTS

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

Memorandum

Subject: INFORMATION: OIG Privacy Audit

Date: August 19, 2008

From: Daniel G. Mintz
Chief Information Officer

Reply to Attn. of:

To: Rebecca C. Leng, Office of the Inspector General

We concur with the OIG findings and all but one recommendation. Regarding the organizational positioning of the Privacy Officer we suggest taking a slightly different approach and suggest we relook where we are next year.

We developed a plan of action to implement the report's recommendations which will help us achieve compliance with OMB requirements for protecting privacy in Federal government agencies. We are in the process of acquiring and implementing technology to assist the Department in protecting the PII within the Department's information technology systems and infrastructure. Specific responses to each of the report's nine (9) recommendations follow:

OIG Recommendation 1: Require system owners to submit evaluation results on whether PII exists in the 320 systems that were not included in the DOT Privacy Office inventory.

OCIO Response: Concur. In August 2007, all DOT systems were evaluated through the Survey of Department of Transportation Systems Containing Personally Identifiable Information. Although this survey was comprehensive and included all DOT systems, during the course of the contractor review, the Office transitioned to a new privacy officer and not all records were available for review. These records have now been made available to OIG. OCIO has also initiated additional measures to ensure appropriate oversight of PII. For example, quarterly C&A compliance reviews are evaluated to determine if the system contains PII and if it has a PIA and SORN. In addition, OCIO is considering requiring system owners to conduct a Privacy Threshold Analysis (PTA) to determine, during initial certification and recertification, whether the system contains PII. This information would be reported to OCIO. OCIO has set a target to implement this requirement by the end of March 2009.

OIG Recommendation 2: Require system owners of sampled systems to correct privacy protection deficiencies identified in the areas of missing SORNs, PIAs, and MOU with outside agencies when sharing PII; notify system owners of remaining PII systems to check whether they need to take similar corrective actions.

OCIO Response: Concur. OCIO has achieved considerable progress in this area as a result of this audit and the trend is continuing. OCIO has notified the system owners of any missing or outdated SORNs and PIAs. OCIO will take action to notify all owners of systems of PII to address and update memoranda of understanding with outside agencies. This recommendation will be fully implemented by the end of March 2009.

OIG Recommendation 3: Require OA Privacy Officers to implement a process under which future systems are subject to periodic review to ensure that SORNs are initiated and posted, PIAs are developed, and MOU with outside agencies are documented: and that such elements are appropriately updated when systems undergo change.

OCIO Response: Concur. The recommended actions coincide with DOT's privacy policy. This recommendation will be implemented through appropriate direction to operating administration CIO's and Privacy Officers, and in DOT CIO Policy by the end of March 2009.

OIG Recommendation 4: Encrypt all PII data transmitted over the Department's communications network.

OCIO Response: Concur. OCIO agrees with the requirement to encrypt all PII data communications. OCIO is presently planning to conduct a detailed analysis of systems and encryption requirements and anticipates that this analysis will be completed by the end of March 2009. At that time, OCIO will detail an action plan to implement encryption requirements consistent with the results of the analysis.

OIG Recommendation 5: Require system owners of sampled systems to correct security deficiencies concerning password security controls, invalid log-in attempts, and sessions time-out expiration; and notify system owners of remaining PII systems to check whether the need to take similar corrective actions.

OCIO Response: Concur. We anticipate that the systems with PII can be secured by the end of July 2009. We will address the issues identified in the report to OA CIOs, ISSOs, Privacy Officers, System Owners and other responsible parties.

OIG Recommendation 6: Require OA Privacy Officers to implement a process under which periodic performance checks are carried out to ensure that all PII systems remain in full compliance with DOT security policies.

OCIO Response: Concur. OCIO will initially issue a Directive by the end of Q1 FY2009 that identifies OCIO's expectations for conducting performance checks to remain in full compliance with security policies. A final policy memorandum will incorporate feedback obtained in the Directive phase, and will be issued by the end of Q2 FY2009.

OIG Recommendation 7: Require system owners of sampled systems to correct security deficiencies found in their Web sites and notify system owners of remaining PII systems to check whether they need to take similar corrective actions.

OCIO Response: Concur. OCIO will provide written notification to the modal Privacy Officers and owners of sampled systems to correct security deficiencies found in their Web sites. OCIO will also direct modal Privacy Officers, ISSO's, and CIO's to work with the owners of all systems to identify necessary corrective actions and develop corrective plans by the end of Q2 FY2009.

OIG Recommendation 8: Provide enhanced privacy security training for OA Privacy Officers, who are responsible for implementing annual privacy practices in their respective organizations.

OCIO Response: Concur. We have recommended specialized training available to OA Privacy Officers. OCIO will establish specialized training requirements – both content and frequency – in written policy by the end of Q2 FY2009.

Appendix B. Management Comments

OIG Recommendation 9: Increase the visibility of the DOT Privacy Program by having the Departmental Privacy Officer report directly to the Chief Information and Privacy Officer

OCIO Response: Concur in part - The tradeoff between following this recommendation and keeping the Privacy Officer in its current organizational location is between increased visibility and the synergies that we believe exists for many of the privacy goals and security goals and implementation plans as well as the ability to make more efficient use of staff collectively.

It is not entirely clear to us how many of the issues identified in the report are due to the personnel changes that were going on during the time of the analysis and thus, how much making this one change, would achieve. We propose leaving the structure as is for the next year – fiscal year 2009, focusing on implementing the suggested changes, enhancing a number of associated internal auditing reviews, and developing more transparent measurements of status. At the end of FY2009, we will relook the status, evaluate how well the office is doing, and determine whether an organizational change would be a good step.

Appendix B. Management Comments