U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary (OST)
Departmental Office of Civil Rights (DOCR)
General Support System (GSS)

Responsible Official

Frederick Ford
Associate Director, S-31
202-366-1785
Frederick.Ford@dot.gov

Approval and Signature

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
Date: 2021.04.07 21:26:55 -04'00'

Executive Summary

The U.S. Department of Transportation (DOT) Departmental Office of Civil Rights (DOCR) established an enterprise-wide cloud-based web-enabled General Support System (GSS) to process discrimination complaints filed against the DOT under Titles VI and VII of the Civil Rights Act of 1964, 42 U.S.C. 2000d et seq, 42 U.S.C. 12101 et.seq, Civil Rights Act of 1991, American with Disabilities Act of 1991, and Genetic Information Nondiscrimination Act of 2008 (GINA). DOCR also processes complaints under 49 CFR Part 23, Disadvantaged Business Enterprise in Airport Concessions and 49 CFR Part 26, Participation by Disadvantaged Business Enterprises in the Department of Transportation Financial Assistance Programs.

The GSS consists of three applications that accept and process the filing of formal complaints and provide a repository for case tracking and management of disadvantaged business enterprise appeals, civil right complaints, and reasonable accommodations requests. The system is also used to generate reports requested by various Federal agencies on civil rights matters, and track investigations and complaint resolution activities involving DOT organizations allegedly engaged in discriminatory practices. This Privacy Impact Assessment (PIA) is required under the EGovernment Act of 2002 because the system collects personally identifiable information (PII) from members of the public and Department employee who 1) file a discrimination complaint, 2) are witness to an alleged discriminatory act, or 3) are alleged to have committed a discriminatory act under Title VII.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The Departmental Office of Civil Rights (DOCR) enforces civil rights laws and regulations, which prohibit workplace discrimination based on race, color, national origin, sex, disability, religion and age in employment and the provision of government services. The GSS contains multiple, integrated sub-systems that help DOCR managers with various administrative support capabilities. These include data entry, tracking, storing and reporting information and are critical in helping the managers evaluate complaints from within the DOT, discrimination complaints generated from the public, and discrimination complaints from the Federal Aviation Administration (FAA) employees. The GSS application accepts and processes the filing of formal complaints and provides a repository for case managers to track and manage such cases. This is accomplished in the DOCR General Support System (GSS) applications hosted in the Tyler Federal (formerly MicroPact Engineering) cloud as follows:

Entellitrak

Entellitrak is a (Software -as-a- Service: SaaS) is used to support the processing of Title VI applications submitted by private sector entities for Disadvantaged Business Enterprise (DBE) status. Application submission is managed through DOT Drupal environment. This application allows DOCR to ensure recipients of funds from the Department of Transportation (DOT) conduct their Federal assisted programs and activities in a non-discriminatory manner and in accordance with United States civil rights laws and labor laws.

The Department's DBE and Airport Concessions Disadvantaged Business Enterprise (ACDBE) website hosts a database that is required by the Department's January 28, 2011, rulemaking, 49 CFR Part 26, Participation by Disadvantaged Business Enterprises in Department of Transportation Financial Assistance Programs. This rulemaking specifically requires Unified Certification Programs (UCP)2 to enter into a database the name, owner, type or action, date of action and reason of action for DBE or

ACDBE firms that have been denied DBE certification. The database helps DBE participants avoid redundancy by determining which firms have been denied certification as DBEs/ACDBEs. The DBE/ACDBE database was developed under DOT standards and is also in conformance with the requirements of the Office of Management and Budget (OMB), Equal Employment Opportunity Council (EEOC), and Congress.

DOT Civil Rights personnel use the contact information, identification information, and descriptive details to document, investigate, and respond to civil rights complaints, inquiries, and DBE appeals, and to conduct reviews of Federally-funded recipients to assess their compliance with civil rights laws. In DBE appeal cases, DOT/DOCR staff use financial information when necessary to make personal net worth determinations about sole proprietors claiming DBE status. PII is received through an initial interview with an investigator, either from the individual directly or through the interview about another individual involved in the complaint. Authorized Civil Rights personnel in each Operating Administration enter data into the system and are responsible for the accuracy of this data.

iComplaints

iComplaints (SaaS) is used to support the submission and processing of complaints made by DOT employees for alleged violations of Title VII, employment discrimination. Complaints are initiated through oral communication, email, and written and supporting documentation and is entered into the system only by DOCR staff. DOCR is responsible for ensuring that DOT does not discriminate against its employees or applicants for employment, and DOT conducts its programs and activities free of discrimination. Major statues which DOCR enforces include: Title VII of the Civil Rights Act of 1964, as amended; Section 504 of the Rehabilitation Act of 1973, as amended; Title II of the Americans with Disabilities Act of 1990; the Equal Pay Act of 1963; Age Discrimination in Employment Act of 1967, and Genetic Information Nondiscrimination Act of 2008 (GINA).

In order for DOCR to record, track, manage, investigate, and report on discrimination complaints, the system collects and stores PII that includes individual's name, mailing address, telephone number, and the last four digits of the social security number. DOCR GSS does not interface with any internal or external systems and does not publicly post any PII information. PII collected by DOCR GSS is not used in any manner that is not specified in notices and is only used for the purposes collected. Only Civil Rights personnel access and use PII in the GSS.

and applicants for employment. Request for accommodation is initiated through oral communication, written requests and email, including any supporting documentation, which is entered into the system only by DOT staff. With respect to disability in the workplace, the DOCR office also has jurisdiction over some entities that do not receive Federal funds. The system enforces compliance with Executive Order 13164, Establishing Procedures to Facilitate the Provision of Reasonable Accommodation.

PII collected in the system consists of: employee's or applicant's name, functional limitation caused by the disability, reasonable accommodation (RA) requested, explanation of how RA would assist the applicant in the application process or the employee in performing his/her job or receiving the benefits and privileges of employment, dates when the required interactive discussions were held, notes from discussion regarding the request, action by deciding official, whether medical documentation was sought, justification for requesting medical documentation, any sources of technical assistance that were consulted, and if the request was denied, the reason for denial (but not medical documentation, which will be kept in a separate file).

Non-PII in the system includes: The employee's or applicant's occupational series and grade or pay equivalent, operating administration, division or office, position title, office location and address and office telephone number; and the deciding official's name, title and office telephone number.

Records in the system are retrieved by date of the reasonable accommodation request, the name of the deciding official, the name of the employee or employment applicant's name, record number, and operating administration or office.

DOCR GSS does not interface with any internal or external systems and does not publicly post any PII information. PII collected by DOCR GSS is not used in any manner that is not specified in notices and is only used for the purposes collected. Only Civil Rights personnel access and use PII in the GSS. In addition, DOCR may share PII through system-generated reports with administrative judges, Federal court judges, attorneys, and others involved with a discrimination complaint. GSS system administrators and authorized personnel in each Operating Administration have access to complaint information containing PII.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

Information is collected in the *Individual Employment Discrimination Form (iComplaints*), OMB number 2105-0556, includes the user's race, religion, and gender, including name, mailing address, telephone number, and partial Social Security Number (SSN).

The name, mailing address, and telephone number are used to contact the complainant, if needed. The last four digits of the SSN is used to create a unique ID for the complainant in the system. Race, religion, and gender are collected if it is related to the complaint. The system can search for complaints by name, mailing address, telephone number, unique ID (created from partial SSN), race, religion and gender. Only name, race, religion and gender are used in internal reports.

Records in each system is retrieved by personal identifier associated with an individual and protected under the Privacy Act. Records covering the primary purpose of the system maintained in accordance with each system of records notice (SORN) are as follows:

- **Entellitrak**: DOT-AL, 24 Departmental Office of Civil Rights System 76 FR 71108, November 16, 2011
- **iComplaints**: DOT-ALL 24 Departmental Office of Civil Rights System, 76 FR 71108, November 16, 2011 and EEOC/GOVT–1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records 67 FR 49354, July 30, 2002
- **RAMS**: DOT/ALL 20, On-line Accommodation Tracking System (OATS), 74 FR 46637, September 10, 2009

An exemption is claimed under DOT/ALL 24, Departmental Office of Civil Rights System pursuant to subsection (k)(2) of the Privacy Act (5 U.S.C. 552a), because this system contains investigatory material compiled for law enforcement purposes. A final rule has been published for DOT/ALL 24 in the DOT Privacy regulations (49 CFR Part 10), Appendix A, to exempt this system from the requirements of the following Privacy Act subsections, for the reasons stated in the proposed revision: (c)(3) (Accounting of Certain Disclosures), (d) (Access to Records), (e)(4)(G), (H), and (I) (Agency Requirements), and (f) (Agency Rules) to the extent that DOCR GSS contains investigatory material compiled for law enforcement purposes.

An exemption is claimed under EEOC/GOVT-1, Equal Employment Opportunity in the Federal Government Complaint and Appeal Records, pursuant to subsection (k)(2) of the Privacy Act (5 U.S.C. 552a), because this system contains investigatory material compiled for law enforcement purposes.

The EEOC has codified its exemptions for this SORN at 29 CFR 1611.13 this system of records is exempt from subsections (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f) of the Act.

As required by the Privacy Act of 1974, a Privacy Act Statement informing applicants of the Departments privacy practices regarding collection, use sharing, safeguarding, maintenance, and disposal of PII is included in all applicable paper and web-based forms, DOT Form, 1050-8, Individual Complaint of Employment Discrimination, OMB approval number 2105-0556.

Individual Participation and Redress

DOT should provide a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision making process regarding the collection and use of their PII and be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Under the provisions of the DOT's Privacy Act/Freedom of Information Act (FOIA) procedures, individuals may request searches of DOCR GSS to determine if any records have been added that may pertain to them. The Freedom of Information Act (FOIA) is a Federal law that gives you the right to access any U.S. Department of Transportation (DOT) records unless DOT reasonably foresees that the release of the information in those records would harm an interest protected by one or more of the nine exemptions (such as classified national security, business proprietary, personal privacy, investigative documents) or release is prohibited by law. The DOT will review all Privacy Act requests on an individual basis and may waive exemptions if the release of information to the individual would not cause harm to applicable exemptions such as law enforcement or national security.

Notification procedure: Individuals wishing to know if their records appear in this system may inquire in writing to the system manager:

Frederick Ford
Office of Civil Rights
1200 New Jersey Ave., SE
E31-312
Washington, DC 20590
Email: Frederick.Ford@dot.gov
Phone: (202) 366-1785

Included in the request must be the following:

- Name,
- Mailing address,
- Phone number or email address,
- A description of the records sought, and if possible, the location of the records.

Contesting record procedures: Individuals wanting to contest information about them that is contained in this system should make their requests in writing, detailing the reasons for why the records should be corrected. Requests should be submitted to the attention of the OST official responsible for the record at the address below:

Claire W. Barrett
Departmental Privacy Officer
1200 New Jersey Ave., SE
E31-312
Washington, DC 20590
Email: privacy@dot.gov
Fax: (202) 366-7024

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

Information collected in DOCR-GSS is used to process discrimination complaints and enforce civil based on race, color, national PII in the DOCR GSS is used by authorized DOT personnel to investigate discrimination complaints and create yearly and quarterly reports to meet Federal reporting requirements. During the investigation process, DOT may use the GSS PII to contact individuals, research facts, and pass on appropriate information to judges, attorneys, and other parties directly involved in the investigation, but only on a need-to-know basis.

- action, date of action and reason of action for DBE or ACDBE firms that have been denied DBE certification to document, investigate, and respond to civil rights complaints, inquiries, and DBE appeals, and to conduct reviews of Federally-funded recipients to assess their compliance with civil rights laws. Financial information may be used when necessary to make personal net worth determinations about sole proprietors claiming DBE status. Information in Entellitrak is collected pursuant to; 49 CFR Part 23, Participation of Disadvantaged Business Enterprise in Airport Concessions and 49 CFR Part 26, Participation by Disadvantaged Business Enterprises in the Department of Transportation Financial Assistance Programs
- **iComplaints** collects, uses and maintains the following PII: individual's name, mailing address, telephone number, and the last four digits of the social security number. The PII in the system is used to ensure compliance that DOT does not discriminate against its employees or applicants for employment, and its programs and activities are free of discrimination.

- **RAMS** collects, uses, and maintains the following PII: employee's or applicant's name, functional limitation caused by the disability, reasonable accommodation (RA) requested, explanation of how RA would assist the applicant in the application process or the employee in performing his/her job or receiving the benefits and privileges of employment, dates when the required interactive discussions were held, notes from discussion regarding the request, action by deciding official, whether medical documentation was sought, justification for requesting medical documentation, any sources of technical assistance that were consulted, and if the request was denied, the reason for denial (but not medical documentation, which will be kept in a separate file).

The following legal authorities allow information to be collected and maintained in both iComplaints and RAMs:

- Title VI and VII of the Civil Rights Act of 1964, as amended;
- Section 504 of the Rehabilitation Act of 1973, as amended;
- Title II of the Americans with Disabilities Act of 1990;
- Equal Pay Act of 1963
- Age Discrimination in Employment Act of 1967
- Executive Order 13164, Establishing Procedures to Facilitate the Provision of Reasonable Accommodation.
- Genetic Information Nondiscrimination Act of 2008 (GINA).

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

Only Civil Rights personnel access and use PII in the GSS. In addition, DOCR may share PII through system-generated reports with administrative judges, Federal court judges, attorneys, and others involved with a discrimination complaint. By law DOT is required to conduct investigations on complaints of discrimination. PII in the DOCR GSS is used by authorized DOT personnel to investigate discrimination complaints and create yearly and quarterly reports to meet Federal reporting requirements. The following retention schedules apply to data in the DOCR GSS application:

DOT submitted a proposed record schedule (DAA-0398-2019-0008a) for **Entellitrak** records to NARA for approval. The following record sets are maintained in Entellitrak and will be maintained as permanent records until the records schedule is approved by NARA:

- Disadvantaged Business Enterprise Division Appeals - DAA-0398-2019-0008-0001, Temporary, Destroy/delete 6 years after cutoff date unless needed longer for business use.

- Affirmed Denials/De-certifications, DAA-0398-2019-0008-0002, Temporary, Destroy/delete 6 years after cutoff date unless needed longer for business use.
- Remand or Reversed Denials/De-certifications, DAA-0398-2019-0008-0003, Temporary, Destroy/delete 6 years after cutoff date unless needed longer for business use.
- Untimely Appeals, DAA-0398-2019-0008-0004, Temporary, Destroy/delete 6 years after cutoff date unless needed longer for business use.
- Challenged Appeals, DAA-0398-2019-0008-0005, Temporary, Destroy/delete 6 years after cutoff date unless needed longer for business use.
- Certificates of Records Destruction, DAA-0398-2019-0008-0006, Temporary, Destroy/delete 6 years after cutoff date unless needed longer for business use.

iComplaints, records are maintained in accordance GRS 2.3, Employee Relations Records, EEO discrimination complaint case files;

- Item 110: Informal Process: Temporary. Destroy 3 years after resolution of case, but longer retention is authorized if required for business use.
- Item 111- Informal Process: Temporary. Destroy 7 years after resolution of case, but longer retention.

RAMS, records are maintained in accordance with GRS 2.3, Employee Relations Records. Reasonable accommodation case files, item 20, Temporary. Destroy 3 years after employee separation from the agency or all appeals are concluded whichever is later, but longer retention is authorized if required for business use.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

During the investigation process, DOT may use the PII maintained in the GSS applications to contact individuals, research facts, and pass on appropriate information to judges, attorneys, and other parties directly involved in the investigation, but only on a need-to-know basis. DOCR does not use the PII for any other purpose. DOCR GSS collects PII and this information is not used in any manner that is not specified in the identified system or records notices and is only used for the purposes collected. DOCR does not publicly post any PII information.

Only Civil Rights personnel access and use PII in the GSS. In addition, DOCR may share PII through system-generated reports with administrative judges, Federal court judges, attorneys, and others involved with a discrimination complaint. GSS system administrators and authorized personnel in each Operating Administration have access to complaint information containing PII.

Records covered under DOT-ALL–24 Departmental Office of Civil Rights System may be disclosed outside of DOT as a routine use pursuant to 5 U.S.C. 552a(b)(3), as follows:

- To the United States Department of Justice (DOJ), including United States Attorneys Offices, or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: 1) DOT or any component thereof; 2) Any employee of DOT in his/her official capacity; 3) Any employee of DOT in his/her individual capacity where the DOJ or DOT has agreed to represent the employee; or 4) the United States, or any agency thereof, is a party to the litigation or has an interest in such litigation and DOT determines that the records are both necessary and relevant to the litigation and the use of such records is compatible with the purpose for which DOT collected the record.
- Additional routine uses for this system can be found in the published Notice.

Records covered under DOT/ALL 20 - On-line Accommodation Tracking System (OATS), 74 FR 46637, September 10, 2009 may be disclosed outside of DOT as a routine use pursuant to 5 U.S.C. 552a(b)(3), as follows:

- To a congressional office from the record of an individual in response to an Inquiry from the congressional office made at the request of the individual.
- To an authorized appeal grievance examiner, formal complaints examiner, administrative judge, equal employment opportunity investigator, arbitrator or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee.
- To another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency when the Government is a party to the judicial or administrative hearing.
- Other possible routine uses of the information, applicable to all DOT systems, are published in the **Federal Register** at 65 FR 19476 (April 11, 2000), under ''Prefatory Statement of General Routine Uses'' (available at *http://www.transportation.gov/privacy*).

Records covered under EEOC/GOVT–1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records may be disclosed outside as a routine use as a routine use pursuant to 5 U.S.C. 552a(b)(3), as follows:

- To disclose pertinent information to a federal, state, or local agency or third party as may be appropriate or necessary to perform the Commission's functions under the Age Discrimination in Employment Act or Equal Pay Act.
- To disclose information contained in these records to state and local agencies administering state or local fair employment practices laws.

- To disclose non-confidential and non-privileged information from closed ADEA/EPA case files (a file is closed when the Commission has terminated its investigation and has decided not to sue) to the employer where a lawsuit has been filed against the employer involving that information, to other employees of the same employer who have been notified by the Commission of their right under 29 U.S.C. 216 to file a lawsuit on their own behalf, and their representatives.
- This list of routine uses is not all inclusive. Additional routine uses applicable to this system can be found in the published Notice.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

PII submitted in Entellitrak, iComplaints and RAMS is collected directly from the individual through initial interview, by form, verbally, email, written complaint, and additional documents submitted by the subject. Authorized users of the system are responsible for ensuring accuracy and completeness of the information entered into the systems.

PII and data information that is collected directly from the individual is submitted into the DOCR-GSS modules by Civil Rights staff only. DOCR staff are responsible for following-up with individuals to ensure the accuracy of the information received for processing and maintained in the DOCR-GSS modules. Access is restricted to only authorized staff and the system maintains audit trails on records access to the system. Mechanisms are in place to restrict access to the system.

Security

DOT shall implement administrative, technical, and physical measures protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

DOT technical support and information security personnel apply security standards, including but not limited to routine scans and monitoring, back-up activities, and background security checks of technical employees and contractors to safeguard PII data in the DOCR GSS. DOCR GSS employs the least privilege rule based on roles and responsibilities to minimize the exposure of PII to personnel who are authorized and have a need-to-know based on job role and function.

DOT CIO and DOCR implements an incident-handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; coordinates incident-handling activities with contingency planning activities; and incorporates lessons learned from ongoing incident handling activities into incident-response procedures, training, and

testing/exercises; and implements the resulting changes DOT has deployed intrusion detection / prevention and firewall devices throughout the network to protect the network from many of the malicious codes. DOT staff and contractors are trained on their roles and responsibilities during incident response activities.

Antivirus software is utilized for malicious code protection on systems where real-time scans on media are performed. A full system scan is performed on a weekly basis and virus definitions are automatically updated on all servers and all the clients.

DOT employees are required to adhere to information system security controls Access for all GSS users must be granted by an administrator, who also sets privileges.

DOCR GSS Rules of Behavior documents are in place that outline specific guidelines for usage of information systems and acknowledge that GSS users understand their roles and responsibilities relative to system access and usage. In accordance to the DOT Order 1351.37 Departmental Cybersecurity Policy, the System Owner for the DOCR GSS has established the procedures needed to adhere to security controls and ensure that all employees and contractors receive annual security training. Training is now available via CBT and results are stored in a database. The various Operating Administration Information Systems Security Managers (ISSM) review training records for compliance by DOT users. DOT Security Awareness Training is administered and maintained through the Training Management System (TMS). All users of DOCR GSS are required to comply with DOT 1351.18, Departmental Privacy Risk Management Policy.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

As determined by the System Owner, Information Systems Security Manager, or the Cybersecurity Management Center (CSMC) at DOT, information security personnel conduct periodic DOCR GSS system audits to ensure logs are reviewed for any anomalies. Only authorized system, database, and application administrators have rights sufficient to access audit logs based on their particular roles. The logged auditable events are adequate to support after-the-fact investigations based on previous requests made by the CSMC.

DOCR GSS Rules of Behavior documents are in place that outline specific guidelines for usage of information systems and acknowledge that GSS users understand their roles and responsibilities relative to system access and usage.

Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual Security and privacy awareness training as well as the DOT/OST Rules of Behavior. The OST Information System Security Officer and OST Privacy Officer will conduct periodic security and privacy

compliance reviews of the CCMS consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b (3), Securing Agency Information Systems.

Responsible Official

Frederick Ford
Director, Departmental Office of Civil Rights (S-31)
202-366-1785
Frederick.Ford@dot.gov

Approval and Signature

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer