



U.S. Department of Transportation

**Privacy Impact Assessment
Federal Aviation Administration (FAA)
Office of Finance and Management (AFN)
Customer Service Center System (CSCS)**

Responsible Official

Dewayne Harp

Email: Dewayne.harp@faa.gov

Phone Number: 405-954-7343

Reviewing Official

Karyn Gorman

Chief Privacy Officer

Office of the Chief Information Officer

privacy@dot.gov





Executive Summary

Customer Service Center System (CSCS) is a Federal Aviation Administration (FAA) Office of Finance and Management (AFN) Information Technology (IT) service management (ITSM) software ticket tracking system combined with follow-up questionnaire functionality and a reports repository providing an efficient, cost-effective set of tools for aiding the staff of the Customer Service Center (CSC) Service Desk and infrastructure administrators. CSCS is a FedRAMP authorized ServiceNow Software as a Service (SaaS) application (ServiceNow). The system is authorized under 49 United States Code (U.S.C.) § 322, 40122(g), 44 USC 3501-3521; 5 CFR Part 1320 and 40101; 40 U.S.C. § 1441 and 486c; 5 U.S.C. § 302.

This Privacy Impact Assessment (PIA) is developed in accordance with Section 208 of the [E-Government Act of 2002](#), because CSCS maintains Personally Identifiable Information (PII) on members of the public (employees and contractors from Federal agencies outside of the DOT, and members of the public).

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 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:

¹Office 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).



- *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 PLA, 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

CSCS is authorized under 49 United States Code (U.S.C.) § 322, 40122(g), 44 USC 3501-3521; 5 CFR Part 1320 and 40101; 40 U.S.C. § 1441 and 486c and 5 U.S.C. § 302 and is an AFN software ticket tracking system combined with follow-up questionnaire functionality and a reports repository providing an efficient, cost-effective set of tools for aiding the staff of the CSC Service Desk and infrastructure administrators.

CSCS, a ServiceNow FedRAMP SaaS, is hosted in the authorized FedRAMP High SaaS which is deployed in the Government Community Cloud (GCC). CSCS is used to manage IT services including service requests, incident management, problem management, change management, knowledge management, service portal, reporting and dashboards, performance analytics, and vulnerability management.

Typical transactions within CSCS include:

- There is helpdesk functionality for members of the public that apply for a federal job through the government website www.USAJOBS.gov. When they apply for a job on the site, but run into an issue, such as creating a USAJOBS account profile, they call the CSCS helpdesk number listed on the USAJOBS website and a CSCS helpdesk technician collects their name, email address, and phone number. The CSCS service desk technician then opens a helpdesk ticket in ServiceNow for the USAJOBS staff to contact the individual. Once the USAJOBS staff receive the notice of a ticket, they open the ticket and call or email the individual. The call portion of the process is outside of the CSCS, and no data is added to the ticket about the individual. Once the USAJOBS staff complete their process they close the ticket in ServiceNow. The records are maintained in CSCS.
- There is helpdesk functionality for Federal employees and contractors from the DOT/FAA or other federal agencies outside of the DOT that have access to ServiceNow based on their preassigned roles as system administrators. If these above individuals run into an issue or the individual notices an issue with their system, they



log into ServiceNow and create a helpdesk ticket. They can also call CSCS customer service phone number for assistance. Federal employees and contractors from federal agencies outside of the DOT accounts are created via a bulk request email from their Access Control Officer (ACO), or an individual request from the ACO. The PII for the accounts is collected by the outside agency ACO and provided for access to ServiceNow.

- There is a feedback questionnaire functionality within the system. CSCS emails a simple customer service feedback questionnaire link out to some internal FAA customers after the completion of the helpdesk ticket. Surveys are sent to random users daily when their helpdesk tickets are closed. They contain only customer username and email address to allow follow-up from CSCS if the user requests follow up. The customer service feedback surveys data is kept in the Helpdesk Survey database within CSCS.

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) v3², 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

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.

³ <https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final>



CSCS is a privacy-sensitive system because it collects and maintains PII (name, email address, and phone number) from members of the public to provide helpdesk services. A Privacy Act Statement (PAS) discussing the Department's privacy practices regarding the collection, use, sharing, maintenance, and disposal of their PII is provided by the Agency/Department at the initial point of collection. The Department also provides general notice to the public of these records collection through the following Privacy Act System of Records Notices (SORN):

- [DOT/ALL 13 Internet/Intranet Activity and Access Records 67 FR 30757 \(May 7, 2002\)](#) covers records and reports including Internet/Intranet Protocol (IP) address of the computer used to make the Internet/Intranet connection, logs of Internet/Intranet access and use from a DOT computer generally do not directly contain names or similar personal identifiers. However, for official government business purposes and through research or investigation, an individual whose PC was assigned an IP address at a given time may be identifiable by name. The records may include the following PII about students: name, email address, phone number, and home address.

The publication of this PIA demonstrates DOT's commitment to providing appropriate transparency into the CSCS system.

Individual Participation and Redress

DOT provides 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 they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

For all inquiries related to the information contained in CSCS the individual may appear in person, send a request via email (privacy@faa.gov), or in writing to:

Privacy Office
800 Independence Avenue, SW
Washington, DC 20591

The request must include the following information:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records
- A signed attestation of identity

If you have comments, concerns, or need more information on FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1 (888) PRI-VAC1.



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. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

Congress has authorized the FAA Administrator to develop systems and/or tools to support business needs for assisting individuals needing customer service. CSCS addresses the unique demands of the FAA's workforce and operates under the authority of 49 United States Code (U.S.C.) § 322, 40122(g), 44 USC 3501-3521; 5 CFR Part 1320 and 40101; 40 U.S.C. § 1441 and 486c; 5 U.S.C. § 302.

CSCS maintains members of the public PII (name, email address, phone number). These can be non-government individuals that are applying for a federal job through the government website www.USAJOBS.gov, but run into an issue, such as creating a USAJOBS account profile, and thus need customer service support. Also, members of the public (employees and contractors from Federal agencies outside of the DOT) that are having issues with ESC supported systems, use CSCS for support.

The FAA uses this access information for purposes of creating and validating login credentials, audit trails, and security monitoring for FAA employees and contractors who use the CSCS program and/or manage the system. This use is consistent with the description in the "purpose" section in the applicable SORN [DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 \(May 7, 2002\)](#).

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.

The FAA minimizes its data maintenance, use, and retention in CSCS to the relevant and necessary information to meet its authorized business purpose of providing IT support services to DOT/FAA employees, contractors, and members of the public. Records within the CSCS records are maintained under [National Archives and Record Administration \(NARA\) approved General Retention Schedules \(GRS\) Customer Service Center System/ N1-237-09-11, Item 1](#). These records are temporary and should be cut off at the end of the fiscal year in which the last service activity is completed. Then destroyed/deleted when three years old or when no longer needed for review and analysis, whichever is later. Information technology operations and maintenance records in CSCS are maintained under [NARA GRS 3.1](#). These records are temporary and should be destroyed three years after help desk tickets are completed and after agreement, control measures, procedures, project, activity, or transaction is obsolete,



completed, terminated or superseded, but longer retention is authorized if required for business use. The technical and administrative help desk operational records are covered by [NARA GRS 5.8](#). These are temporary and should be destroyed when business use ceases. Lastly, system access and authentication records are maintained pursuant to [NARA GRS 3.2](#). These records are temporary and can be destroyed when business use ceases.

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.

The FAA limits the scope and collection of PII to what is necessary to meet business needs of the program specifically for communicating with individuals needing helpdesk services and creating user accounts.

The FAA/DOT limits the scope of PII collected including:

- First and last name
- Email address
- Phone number

This PII is collected to support the purpose specified in SORN [DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30757 \(May 7, 2002\)](#).

Routine uses include, but are not limited to:

- To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems.
- To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings.
- To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records.
- To other government agencies where required by law.



The Department has also published 15 additional routine uses that apply to all DOT Privacy Act systems of records, including this system. These routine uses are published in the Federal Register at [75 FR 82132, December 29, 2010](#), [77 FR 42796, July 20, 2012](#), and [84 FR 55222, October 15, 2019](#) under "Prefatory Statement of General Routine Uses."

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).

Federal employees and contractors and non-government members of the public, who have applied for a job through www.USAJOBs.gov, provide their information/PII to the CSCS helpdesk technician. Because these individuals provide their PII to CSCS, they are responsible for ensuring its accuracy and it is assumed that the information is correct. The FAA employs processes to ensure the quality and integrity of CSCS data including input validation, which is built into ServiceNow. For example, CSCS automatically checks spelling and has field level validation for input, such as if there is a numerical field, a number is all that can be entered and if there is a date field, a date is all that can be entered. CSCS data are encrypted at rest and in transit. CSCS logs are audited as needed. The audit logs that are generated from the audits are reviewed by business owners to ensure proper use of the system.

Security

DOT shall implement administrative, technical, and physical measures to 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.

The FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020 (includes updates as of Dec. 10, 2020).

These safeguards include an annual independent risk assessment of the CSCS system to test security processes, procedures and practices. The system operates on security guidelines and standards established by NIST and only FAA personnel with a need to



know are authorized to access the records in CSCS. All data in-transit is encrypted and access to electronic records is controlled by Personal Identity Verification (PIV) and Personal Identification Number (PIN) and limited according to job function. Additionally, FAA conducts annual cybersecurity assessments to test and validate security process, procedures and posture of the system. Based on security testing and evaluation in accordance with the FISMA, the FAA issues CSCS an on-going authorization to operate.

The following safeguards are designed to ensure the security, integrity, and confidentiality of PII in CSCS:

- Encryption of PII while stored and/or transmitted is compliant with FIPS 140-2 standards.
- CSCS personnel handling sensitive information are required to undergo appropriate background checks to assess their suitability to perform in public trust positions.
- Additionally, all staff undergoes initial security awareness training and annual refresher training, and the procedures for properly protecting the privacy of users' personal information are stressed in this training.

CSCS operates in accordance with DOT Order 1351.37, Departmental Cybersecurity Policy which requires:

- All DOT information systems that are subject to the Federal Information Security Management Act (FISMA) must undergo continuous monitoring of the security controls of the information system;
- The results of the continuous monitoring are to be reported to the Authorizing Official (AO) on at least an annual basis to communicate any changes in the risk posture of the information system; and
- The AO, with assistance of the Information System Owner (ISO), Risk Executive and other DOT component personnel, review risk posture and planned corrective actions for reducing risk to make a determination if risk is acceptable for continued operation.

CSCS is designed to meet all current cyber security requirements for protecting privacy information while still allowing only authorized users the full transparency needed to complete the personnel security process for applicants, employees, and contractors. CSCS records are safeguarded in accordance with applicable rules and policies, including all applicable Department automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored.

Access to the computer system containing the records in CSCS is limited to those individuals who have a need to know the information for the performance of their official



duties and who have appropriate clearances and permissions. CSCS is protected from unauthorized access through appropriate administrative, physical, and technical safeguards and all system access is logged and monitored.

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.

FAA is responsible for identifying, training, and holding Agency personnel accountable for adhering to FAA privacy and security policies and regulations. FAA Order 1370.121B, “FAA Information Security and Privacy Program & Policy,” implements the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

DOT implements 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.

In addition to these practices, the FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with CSCS are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of CSCS as related to the requirements of OMB Circular A-130, “Managing Information as a Strategic Resource.”

Responsible Official

Dewayne Harp
Information System Owner
Technology Service Management Team Lead, AMK-261

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN
MARIE
GORMAN

Digitally signed by
KARYN MARIE
GORMAN
Date: 2026.09.30
12:35:11 -04'00'