U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Web-based Operations Safety System (WebOPSS)

Responsible Official

Elaine Rodgers
Email: Elaine.Rodgers@faa.gov
Phone Number: 770-383-2801

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Federal Aviation Administration's (FAA) Aviation Safety Organization (AVS) owns and operates the Web-based Operations Safety System (WebOPSS) which operates under Title 49 U.S.C. 332 and 5 U.S.C. 301. WebOPSS is used by the FAA's Flight Standards Service to disseminate FAA requirements to air operators (e.g., air carriers such as airlines) and air agencies (e.g., repair stations, training centers, and pilot schools) and manage authorizing documents. Those authorizing documents require that FAA and aviation industry users have digital certificates so they can electronically sign the documents. The Digital Certificate Service (DCS) within WebOPSS provides those digital certificates.

The FAA is publishing this Privacy Impact Assessment (PIA) under Section 208 of the E-Government Act of 2002. The DCS collects the following Personally Identifiable Information (PII) from aviation industry air operators and air agency employees; their name, social security number (SSN), date of birth (DOB), home phone number, email address, driver's license number and state of issuance, whether the driver's license address is the current address or a previous address, current street address, years at that address, most recent previous address, billing address, indication of whether their credit card is a US card, their credit card number, CVC code, and card expiration year and date. DCS only maintains their name, email, and certificate order ID.

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]

[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).

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:

- *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 creation of a WebOPSS account is recommended, but not necessary, before FAA employees or aviation industry personnel to get a digital certificate from DCS.

Digital Certificate Service (DCS)

DCS is used to purchase digital certificates. DCS resides on an FAA Web server system located at the URL https://dcs.faa.gov/. FAA has contracted with Leidos, Inc. to maintain the DCS website and manage its DCS services. Under Leidos's administration, DCS utilizes external online services as follows:

- Elavon Inc. for Virtual Merchant services (card payment),
- Equifax Inc. via eIDcompare[2], for identity authentication, and
- GlobalSign for issuance of digital certificates and electronic signatures.

DCS has two different paths for purchasing a digital certificate, depending on whether the individual is an FAA employee (Internal User) or an aviation industry person (Industry User).

[2] The WebOPSS program is currently discussing using MyAccess instead of Equifax for identity authentication of U.S. citizens and non-U.S. citizens. A new interface with Equifax must first be implemented, which will not occur before July 2024, before the program can move forward with any change.

Industry Users

Industry Users navigate to https://dcs.faa.gov/ to request a digital certificate, where they are required to read and accept the Digital Certificate Service Subscriber Agreement and read additional notices explaining the authentication process found here. After accepting the agreement, a page is displayed alerting the Industry User that if they have an Identity Protection Service, such as LifeLock, or a consumer-requested security freeze monitoring their credit, they will not be able to complete the online authentication process. If applicable, the Industry User must instead complete a Proof of Identity form which is explained more fully on page 5.

The Industry User is then presented with an opportunity to review an outline of the fees charged for the Digital Signature services by clicking on the Support page link. The Industry User must then click on the "US Resident" link to begin the online application process. If the Industry User clicks on the "Non-US Resident" link, they are presented with instructions for completing a Proof of Identity form.

The Industry User manually enters their name, social security number (SSN), date of birth (DOB), home phone number, email address, driver's license number and state of issuance, whether the driver's license address is the current address or a previous address, current street address, years at that address, and their most recent previous address into the New Certificate Request web form. The Industry User has the optional opportunity to then provide an organizational affiliation which will be included within their digital signature by entering an organization name, city, state, and country. The Industry User is then presented with a screen of their entered data and asked to either verify their information by hitting the "continue" button or using the "edit' button to correct their information. Once the Industry User hits the "continue" button, they are queried again if their entries are accurate.

If the Industry User selects "yes", they are taken to the Credit Card Payment page. The Industry User enters their name, billing address (with the opportunity to note that the billing address is the same as their current street by clicking a box), indication of whether the card is a US card, their credit card number, CVC code, expiration year, and date. The Industry User is advised that after their payment has completed processing, the credit card information is deleted and DCS does not retain their credit card information in DCS files. The Industry User then hits the submit button. The DCS encrypts the Industry User information and sends it first to Elavon, Inc. Once transmitted, the New Certificate Request web form is reset to blank.

DCS sends the encrypted information first to Elavon to perform a check on whether this is a valid credit card. If Elavon determines that it is a valid credit card, then the encrypted information is sent onward to Equifax for the ID check. If the Industry User passes the ID check, then their credit card is charged $35.00 by Elavon. If the Industry User does not pass the ID check, then their credit card is charged $9.50 by Elavon, and the Industry User gets two more attempts within the next 72 hours to try again. If Elavon determines that the credit card is invalid, then the user receives an on-screen message that the credit card transaction cannot be authenticated, and they can then try again.

Equifax returns a pass/fail to DCS regarding the identity authentication. The purpose of this exchange is to validate the individual's identity. Elavon returns to DCS the digital certificate requestor's name, email address, transaction information, date/time stamp of the transaction, whether the transaction was successful, and the transaction amount. The purpose of this exchange is to process payment for digital certificates.

Once the Industry User has had their ID verified and their credit card charged for the transaction, the DCS sends the digital certificate information encrypted in transit to GlobalSign to process the digital certificate, including name, email address, and if provided, Organization Name and location. GlobalSign sends a digital certificate order identification number back to DCS. The purpose of this exchange is to issue a digital certificate to the individual.

When the digital certificate is ready for pick up, the Industrial User receives two different emails. GlobalSign sends the first email from DigitalCertificate@globalsign.com notifying the industry user that the certificate is ready for pickup and includes a one-time download link to the GlobalSign site. The second email is auto generated from afs-webopss@faa.gov and provides a temporary password and instructions on how to retrieve the digital certificate. The Industry User navigates to the link provided in the first email to retrieve their certificate. The Industry User enters the password provided in the second email. The Industry User is required to enter a new password and to also review and accept a GlobalSign Agreement. At that point, the Industry User downloads and saves the digital certificate locally on their computer. The digital certificate includes their name, email address, certificate ID, and organization (if provided).

Industry Users outside the U.S., or U.S. residents that have an identity protection service, such as LifeLock or a consumer-requested security freeze, are not able to complete the authentication process online and will have to complete the *Proof of Identity Form.* The Industry User enters their name, address, company name (optional), email address, telephone number, signature, and photocopy of their Government-Issued Photo Identification (Passport or Driver's License) in the space provided on the Proof of Identify

Form. The Proof of Identity Form must be notarized, and the certifier enters their details that includes name of the Notary Public / Solicitor / Attorney, country, certification purpose and date, signature, and seal. The Industry User mails the Proof of Identify Form to Leidos using the address located on the form. Leidos does not share this information with FAA or Equifax.

Once Leidos processes the Proof of Identity form, Industry Users receive an email notifying them of the successful processing of the form, including a link to complete the purchase of the digital certificate following the previously described process. As soon as the credit card transaction is approved, the digital certificate request is sent directly to GlobalSign.[3] DCS Administrators do not manually request the digital certificate through DCS.

When the digital certificate is ready for pick up, the Industry User receives two different emails. GlobalSign sends the first email from DigitalCertificate@globalsign.com notifying the Industry User that the certificate is ready for pickup and includes a link to the GlobalSign site. The second email is auto generated from afs-webopss@faa.gov and provides a temporary password and instructions on how to retrieve the digital certificate. The Industry User navigates to the link provided in the first email to retrieve their certificate. The Industry User enters the password provided in the second email. The Industry User is required to enter a new password and to also review and accept a GlobalSign Agreement. At that point, the Industry User downloads and saves the digital certificate locally on their computer.

Internal Users

FAA supervisors of Internal Users send an email to the DCS Administrator to request a digital certificate. They provide the employee's name, FAA email, office ID and location. The DCS Administrator logs into https://dcs.faa.gov/ using their username and password and manually enters the FAA employee's information. DCS encrypts and sends the information directly to GlobalSign to issue a certificate.

Unlike Industry Users, digital certificates for FAA Users do not require any communication with Equifax Inc. or Elavon Inc., because FAA employee identity is confirmed by the FAA[4], and certificates are purchased by the FAA, not the employee.

When the digital certificate is ready for pick up, the Internal User receives two different emails. GlobalSign sends the first email from DigitalCertificate@globalsign.com notifying

[3] Leidos has a Purchase Order with Global Sign for the purchase of the license.

[4] FAA employee identity is confirmed by the presence of an active FAA Active Directory (AD) account.

the internal user that the certificate is ready for pickup and includes a link to the GlobalSign site. The second email is auto generated from afs-webopss@faa.gov and provides a temporary password and instructions on how to retrieve the digital certificate.
The Internal User navigates to the link provided in the first email to retrieve their certificate. The Internal User enters the password provided in the second email. The Internal User is required to enter a new password and to also review and accept a GlobalSign Agreement. At that point, the Internal User downloads and saves the digital certificate locally on their computer. The digital certificate includes their name, email address, office ID, and certificate ID.

Renewals

For FAA and Industry users, the digital certificate is valid for one year from the date of issuance. Reminder emails are sent to the FAA user 30 days in advance of the renewal date. If the FAA user does not renew within that 30-day window, they must request a new digital signature. If Industry users cannot renew within the 30 days before the expiration date of their certificate, they must follow procedures outlined above for Industry Users to purchase a new digital certificate. If either a FAA or Industry user needs to change any information on their digital certificate (name, office, etc.) they must apply for a new digital signature using the steps outlined above, not a renewal.

Reports

Two reports can be run by DCS system administration personnel on an as needed basis to research transactions and provide help to users. The Certificate Issuance Report includes: user type (Industry User or Internal User (FAA), first name, middle initial, last name, suffix, email, certificate order ID (this is the “name" of their digital certificate composed of three initials of their name, year of issuance, MM (Month), DD (Day), and six digits, how the certificate was issued (manually versus digitally), status (for instance, if trying to renew, did something fail?), certificate expiration date, amount paid ($35.00, $9.50, or $29.50) and the process date. The Proof of Identity (POI) Report includes name, email, status (complete versus incomplete).

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*[5]*, 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*[6]*.*

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.

DCS system administration personnel have access to the following data with which internal reports are generated to track overall digital certificate processing numbers and transactions. That data includes user type, name, email, the certificate order ID, if the certificate was issued manually or digitally, status of processing, certificate expiration date, amount paid, and the process date. These records are not retrieved by personal identifiers of name or email address. Therefore, the primary records in DCS do not constitute a Privacy Act System of Records.

The issuance of a digital certificate and identity proofing are done by a third party and notice is provided at https://dcs.faa.gov. DCS acts as a pass-through for that information but does not maintain any of the information collected. Before entering their information, digital certificate applicants are presented with a Customer Agreement Form, which they must accept.

The publication of this PIA further demonstrates DOT's commitment to provide appropriate transparency regarding DCS.

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

[5] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

[6] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

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.

Information is collected directly from individuals wishing to purchase a digital certificate by a third party as described in the system overview. Because certain data elements are encrypted within, and are part of the digital certificate, an individual wishing to change any information on their digital certificate such as their name, email address, or organizational affiliation cannot do so. They must instead purchase a new digital certificate or in the case of a FAA user, apply for a new digital signature. For inquiries about changing or renewing their digital certificate information, users can refer to information posted at https://dcs.faa.gov/Support.

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.

WebOPSS) operates under Title 49 U.S.C. 332 and 5 U.S.C. 301. DCS, within WebOPSS, collects PII as outlined in the System Overview from Internal and Industry Users to provide digital certificates so that Internal and Industry users can electronically sign authorizing documents created in WebOPSS. The Government Paperwork Elimination Act (Public Law (PL) 105-277, Title XVII); the Electronic Signatures in Global and National Commerce Act (E-Sign) (PL 106-229); and Office of Management and Budget (OMB) Memorandum M-00-15, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, encourage the use of electronic records, signatures, and alternative information technologies, and allow Government agencies to develop performance standards for their use. OMB Circular A-130, Managing Information as a Strategic Resource, provides general guidance for federal organizations regarding the use of electronic signatures in connection with electronic records and electronic transactions. The use of these electronic technologies also supports the goals of the Small Business Paperwork Relief Act of 2002 (H.R. 327). The FAA’s Advisory Circular AC 120-78A provides guidelines on meeting the FAA’s performance standards developed in accordance with the listed PLs and OMB memorandum.

DCS sends the information outlined in the System Overview encrypted in transit to Equifax, Inc., for identity authentication. Equifax returns a pass/fail to DCS regarding the identity authentication. The purpose of this exchange is to validate the individual’s identity.

DCS sends payment information encrypted in transit to Elavon Inc., a virtual merchant, as outlined in the System Overview. Elavon returns to DCS the transaction information, date/timestamp of the transaction, whether the transaction was successful, and the transaction amount. The purpose of this exchange is to process payment for digital certificates.

DCS sends digital certificate information as outlined in the System Overview encrypted in transit to GlobalSign to process the digital certificate, including name, email address, office code and office location (for FAA user), Organization Name and location (for Industry users), if provided. GlobalSign sends a digital certificate order identification number back to DCS. The purpose of this exchange is to issue a digital certificate to the individual.

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 PII collection, maintenance, use, and retention in DCS to only the information necessary to create digital certificates used for signing authorizing documents. The DCS program is currently exploring the use of MyAccess for identity verification in lieu of its current procedures. This results in the collection of less PII about individuals.

Leidos maintains all hard copies of the Proof of Identity forms received through the mail in a securely locked cabinet for one year; at the end of one year, the forms are destroyed and Leidos sends an email to the FAA point of contact stating when the yearly hard copy of the DCS forms was destroyed.

Leidos historically destroyed the Proof of Identity documents used in the creation of digital certificates for Industry Users.

- Proof of Identity documents processed by Leidos from 2013 to 2020 were destroyed in June 2022.
- Proof of Identity documents processed by Leidos from 2020-2021 were destroyed in January 2023.
- Proof of Identity documents processed by Leidos from 2022 were destroyed in January 2024.

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.

As described in the System Overview section, records in DCS are shared outside of DOT with third parties for the purpose of issuing digital certificates so that FAA employees and contractors and representatives from commercial air operators and air agencies (Industry Users) can digitally sign safety and economic authority documents. Leidos Inc., by virtue of its contract with DOT to manage DCS services, must comply with applicable contract clauses governing privacy and security, ensuring, for instance, that personal data of DCS users will not be sold secondarily. Additionally, the DCS site also contains links to Globalsign's privacy and data policies which further describe how this third party handles personal data.

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).

FAA and third parties have taken reasonable steps to confirm the accuracy of PII used in DCS by collecting information directly from individuals. Because individuals directly input their PII, it is presumed accurate. The web forms used to collect PII from individuals contain warnings cautioning users to enter PII accurately. The web forms implement data validation techniques such as data type checks, range checks, and format checks. For inquiries about changing digital certificate information, users can refer to information posted at https://dcs.faa.gov/Support.

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).

DCS employs specific administrative, technical, and physical measures to protect PII against loss, unauthorized access, or disclosure. All PII is encrypted in transit and at rest. DCS personnel receive guidance on their duties as they relate to collecting, using, processing, and securing PII. This includes mandatory annual security and privacy awareness training, as well as a review of the FAA Rules of Behavior.

The FAA has a privacy/security incident response plan which includes procedures for detection of a privacy/security incident, remediation and response if one occurs, and notification where appropriate to protect and inform impacted individuals. In addition, the FAA conducts annual privacy/security incident response exercises to evaluate the effectiveness of this plan.

WebOPSS/DCS has a system security plan in place. WebOPSS/DCS was issued an Authority to Operate on August 29, 2023, after completing the authorization and accreditation process that reviews security controls and procedures and that validates that WebOPSS/DCS is compliant with appropriate information security processes and policies.

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.

The DOT/FAA 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.

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.

In addition to these practices, the FAA implements additional policies and procedures as needed as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with WebOPSS/DCS 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, as well as FAA Order 1370.121B. The FAA conducts periodic privacy compliance reviews of WebOPSS/DCS as related to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource*.

Responsible Official

Elaine Rodgers
System Owner
Computer Scientist, AFN/FAA

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN

Digitally signed by KARYN MARIE GORMAN
Date: 2024.04.25 11:31:48 -04'00'