Privacy Threshold Assessment (PTA)

Federal Aviation Administration (FAA)
Office of Aviation Safety (AVS)
Web-based Operations Safety System (WebOPSS)

CLAIRE W BARRETT

Digitally signed by CLAIRE W BARRETT
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=CLAIRE W BARRETT
Date: 2018.09.26 20:14:29 -04'00'

9/26/2018

X Claire W. Barrett

Claire W. Barrett
DOT Privacy Office - Adjudicated - 092618
Signed by: OSTHQ

Privacy Threshold Assessment (PTA)

The Privacy Threshold Assessment (PTA) is an analytical tool used to determine the scope of privacy risk management activities that must be executed to ensure that the Department's initiatives do not create undue privacy risks for individuals.

The Privacy Threat Assessment (PTA) is a privacy risk management tool used by the Department of Transportation (DOT) Chief Privacy Officer (CPO). The PTA determines whether a Department system[1] creates privacy risk for individuals that must be further analyzed, documented, or mitigated, and determines the need for additional privacy compliance documentation. Additional documentation can include Privacy Impact Assessments (PIAs), System of Records notices (SORNs), and Privacy Act Exemption Rules (Exemption Rules).

The majority of the Department's privacy risk emanates from its direct collection, use, storage, and sharing of Personally Identifiable Information (PII),[2] and the IT systems used to support those processes. However, privacy risk can also be created in the Department's use of paper records or other technologies. The Department may also create privacy risk for individuals through its rulemakings and information collection requirements that require other entities to collect, use, store or share PII, or deploy technologies that create privacy risk for members of the public.

To ensure that the Department appropriately identifies those activities that may create privacy risk, a PTA is required for all IT systems, technologies, proposed rulemakings, and information collections at the Department. Additionally, the PTA is used to alert other information management stakeholders of potential risks, including information security, records management and information collection management programs. It is also used by the Department's Chief Information Officer (CIO) and Associate CIO for IT Policy and Governance (Associate CIO) to support efforts to ensure compliance with other information asset requirements including, but not limited to, the Federal Records Act (FRA), the Paperwork Reduction Act (PRA), the Federal Information Security Management Act (FISMA), the Federal Information Technology Acquisition Reform Act (FITARA) and applicable Office of Management and Budget (OMB) guidance.

Each Component establishes and follows its own processes for developing, reviewing, and verifying the PTA prior to its submission to the DOT CPO. At a minimum the PTA must be reviewed by the Component business owner, information system security manager, general counsel, records officers, and privacy officer. After the Component review is completed, the Component Privacy Office will forward the PTA to the DOT Privacy Office for final

[1] For the purposes of the PTA the term "system" is used throughout document but is not limited to traditional IT systems. It can and does refer to business activity and processes, IT systems, information collection, a project, program and/or technology, and proposed rulemaking as appropriate for the context of the assessment.

[2] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

adjudication. Only PTAs watermarked "adjudicated" and electronically signed by the DOT CPO are considered final. Do NOT send the PTA directly to the DOT PO; PTAs received by the DOT CPO directly from program/business owners will not be reviewed.

If you have questions or require assistance to complete the PTA please contact your Component Privacy Officer or the DOT Privacy Office at privacy@dot.gov. Explanatory guidance for completing the PTA can be found in the PTA Development Guide found on the DOT Privacy Program website, www.dot.gov/privacy.

PROGRAM MANAGEMENT

SYSTEM name: Web-based Operations Safety System (WebOPSS)

Cyber Security Assessment and Management (CSAM) ID: 1410

SYSTEM MANAGER CONTACT Information:

Name: Jean Mortellaro

Email: jean.mortellaro@faa.gov

Phone Number: 206-231-3293

Is this a NEW system?

☐ **Yes** (Proceed to Section 1)
☒ **No**
☒ **Renewal**
☐ **Modification**

Is there a PREVIOUSLY ADJUDICATED PTA for this system?

☐ **Yes:**

Date:

☒ **No** There is an FAA-reviewed PTA dated 07/27/2010

1 SUMMARY INFORMATION

1.1 System TYPE

☒ **Information Technology and/or Information System**

Unique Investment Identifier (UII): 021-189475443[3]

Cyber Security Assessment and Management (CSAM) ID: 1410

☐ **Paper Based:**

☐ **Rulemaking**

Rulemaking Identification Number (RIN):

Rulemaking Stage:

☐ **Notice of Proposed Rulemaking (NPRM)**
☐ **Supplemental NPRM (SNPRM)**:
☐ **Final Rule**:

Federal Register (FR) Notice: Click here to enter text.

[3] The CSAM UII has not been updated and identifies the system under an old UII code (CSAM UII: 021-615337796).

☒ **Information Collection Request** (ICR)[4] The Federal Aviation Administration (FAA) Paperwork Reduction Act (PRA) Officer has been notified that the Leidos Proof of Identity Form requires PRA approval, as does the Digital Certificate System (DCS) web form. OST Forms 6410 and 6411 have also expired and should be updated.

- ☐ **New Collection**
- ☐ **Approved Collection or Collection Renewal**
  - ☐ **OMB Control Number:**
  - ☐ **Control Number Expiration Date:**

☐ **Other:**

1.2 System OVERVIEW:

This is an update to the Federal Aviation Administration (FAA)-reviewed Privacy Threshold Assessment (PTA) for the Web-based Operations Safety System (WebOPSS). The system is hosted at the Mike Monroney Aeronautical Center, 6500 S MacArthur Boulevard, Oklahoma City, Oklahoma 73169. Since the date of the FAA-reviewed PTA, WebOPSS has undergone significant changes; including major functionality changes for the Digital Certificate System (DCS) component, leading to the addition of significant additional personal identifiable information (PII), including Social Security Numbers (SSN), among other PII data elements. The previous PTA also did not address data sharing; this PTA is updated to describe the internal and external data sharing.

WebOPSS consists of a suite of five applications that support the certification and authorization process for air operators and air agencies[5] to conduct business and fly in the national airspace. The applications are as follows:

1. Web-Based Operations Safety System (WebOPSS) application
2. Digital Certificate Service (DCS)
3. Operations Approval Portal System (OAPS)
4. Operations Safety System Insurance Headquarters (OPSS Insurance HQ)
5. Operations Safety System Exemptions Headquarters (OPSS Exemptions HQ)

During the certification process, air carrier and air operator applicants must submit evidence of qualifications to meet FAA safety standards and, if conducting air transportation, proof of their economic fitness. The conditions and limitations of an air carrier and air operator certificate are authorized through authorizing documents issued through WebOPSS, such as: Operations Specifications (OpSpecs) (a set of conditions and limitations authorized by the FAA and with which an air carrier or air operator must comply); Management Specifications (MSpecs)(used to authorize fractional ownership programs, which are programs of shared aircraft ownership);

[4]See 44 USC 3201-3521; 5 CFR Part 1320

[5] Air operators (e.g. air carriers such as Delta Airlines, United Airlines) and air agencies (e.g. repair stations, training centers, pilot schools) are considered members of the public. 14 C.F.R. Part 119 (for air carriers) and 14 C.F.R. Part 145 (for air agencies).

Training specifications (TSpecs) (authorize training centers to use facilities, equipment, personal and courseware required to conduct training); Letters of authorization (LOA) and waivers (LOAs and waivers are issued by the FAA for specific flight operations).

The certification process is designed so that air operator and air agency programs and technology are thoroughly reviewed, evaluated, and tested. The certification process includes the following five phases[6]: pre-application, formal application, document compliance, demonstration, inspection, and final certification. Only the final certification phase is supported by WebOPSS.

System Access

Each of the five modules within WebOPSS requires authentication. FAA Users request access through their supervisor, who sends a request to the FAA MyIT Help Desk and a ticket is created via the MyITSM ticketing System[7]. The supervisor provides the following PII on the user: name, role/title, organization, FAA email address, telephone number, office code/location, office address and access privileges. This access request is outside WebOPSS boundaries. None of the PII from the form, other than name and email address is entered into WebOPSS. Users are authenticated through their workstation using their Active Directory account and Personal Identity Verification (PIV)[8] card. Once in the application, contents and privileges may vary depending on the user's assigned role. External user access to the various applications will be described in the applicable application.

WebOPSS application

The WebOPSS application is used to process final authorizing documents issued to Industry Users, including OpSpecs, MSpecs, TSpecs, LOAs and waivers. Industry users can participate in this process and utilize over 1,000 templates.

In order to receive a WebOPSS account, Industry Users must receive WebOPSS training. These users may enroll in the Industry WebOPSS course (organized by the FAA Academy[9]). Once training has been accomplished, the Principal Operations Inspector[10] sends a request via email for a WebOPSS account to the FAA MyIT Help Desk, and a ticket will be created via the MyIT Service Management (MyITSM) system . The Principal Operations Inspector will provide the following PII to MyITSM: name and business email address. Training records are not input into WebOPSS.

[6] These five phases are described in FAA Order 8900.1, Volume 2, Chapter 1, Section 1.
[7] The FAA MyIT Help Desk services are part of the MyIT Service Management (MyITSM) system – formerly called the Remedy Action Request System (Remedy). MyITSM has an adjudicated PTA, dated December 27, 2016. An update is currently in development.
[8] The PIV information, such as PIV card serial number, does not transverse the system boundaries of WebOPSS and is not stored in the WebOPSS system.
[9] This process is part of the Instructional Resource Information System (IRIS). The IRIS system has a PTA that is currently pending adjudication at the DOT Privacy Office.
[10] Principal Operations Inspectors are FAA Users and are the liaison between Industry Users and the FAA. Inspectors are responsible for ensuring legal compliance of air carriers and air operations within FAA rules and regulations.

Once the account is created, the applicant receives an email containing a temporary password with instructions to log in and change the temporary password. Industry Users manage their account through the External User Provisioning (EUP) system, which is outside WebOPSS boundaries[11]

WebOPSS displays different available templates that Industry Users and FAA Users can employ to draft and review the authorizing documents. These documents are located in a common workspace available to both users. PII that may be manually input into WebOPSS includes information on FAA Users involved in the approval process: Name, role/title, Organization, FAA email address, Office code/location, address, and information related to Industry Users including name, role/title, organization, address, email address, telephone number, username, aircraft registration number, and certificate status/type/number.

Once the authorizing document is reviewed and approved by the FAA, the document is digitally signed in WebOPSS using the digital certificate obtained through the DCS – explained below.

DCS application

DCS is an online application that is used by FAA (authorized FAA Inspectors, Supervisors and Managers) and Industry Users to purchase digital certificates[12] in order to enable these individuals to digitally sign authorized documents in WebOPSS. DCS resides on an FAA Web server system located at the URL https://dcs.faa.gov/. [13]DCS accesses external online services including Elavon Incorporated for Virtual Merchant services (card payment), Equifax Inc. via eIDcompare[14] for identity authentication, and the certification authority GlobalSign for digital certificate issuance[15]. Leidos, Inc., who the FAA has contracted with to manage the DCS services, has a Task Order with the FAA, and Purchase Orders for licenses with Elavon, Equifax and GlobalSign.

DCS has two different processes for purchasing a digital certificate, depending on whether the individual is an FAA User or an Industry User.

FAA Users

Only designated FAA Users are able to apply for a digital certificate for use in WebOPSS. The supervisor should send a request to the DCS Administrators via email (AFS-WebOPSS@faa.gov) providing the following PII of the individual needing the

[11] This portal is part of the FAA DS.
[12] A digital certificate is an electronic credential that allows a person, computer, or organization to exchange information securely over the Internet and to electronically sign documents using the Public Key Infrastructure (PKI).
[13] The DCS home page needs to be updated to include a statement as to its collection of PII.
[14] eIDcompare is an Internet-based service that helps companies mitigate the risk of doing business online, by validating that an applicant's identity actually exists or by verifying the identity of a joint applicant not present during an account opening process.
[15] Leidos Inc. is the provider who maintains the DCS website. The FAA has contracted with Leidos Inc. under National Airspace System Integration Support Contract (NISC) to provide turnkey solutions for DCS. FAA does not have a direct relationship with the third parties. Leidos has Purchase Orders for licenses from Equifax and GlobalSign.

certificate: name, FAA email address, office, location. FAA Users are unable to utilize their PIV cards for digital signature, as WebOPSS was not built to utilize that technology. Updating the functionality to utilize PIV cards would be cost prohibitive.

As soon as DCS Administrators receive the request, they will generate the digital certificate by navigating to the site https://dcs.faa.gov/ and using their Administrator credentials (username and password). Once in the system, DCS Administrators manually enter the following PII: name, FAA email address, office, and location. This information is then transferred to GlobalSign.

After the information is successfully submitted, the FAA User will receive a "certificate request in progress" email. When the digital certificate is ready for pick up, the FAA User will receive 2 different emails, one from DigitalCertificate@globalsign.com notifying that the certificate is ready for pickup and including a link to the GlobalSign site, and another one from afs-webopss@faa.gov providing a temporary password necessary to retrieve the digital certificate.

To retrieve the digital certificate, FAA Users navigate to the GlobalSign link provided in the first email and enter the pickup password provided in the second email from DCS. Once submitted, they are required to enter a new password and to also review and accept a GlobalSign Agreement. At that point, FAA Users will be able to download and save the digital certificate locally on their computer. The digital certificate will include their name and certificate ID.

Unlike Industry Users, digital certificates for FAA Users do not require any communication to Equifax Inc. or Elavon Inc., as the FAA employee identity is confirmed by the FAA, and certificates are purchased by the FAA, not the employee.

Industry Users

Industry Users can request a digital signature for use within WebOPSS by navigating to https://dcs.faa.gov/ where they will be required to read and accept the Digital Certificate Service Subscriber Agreement and additional notices explaining the authentication process.

After accepting the agreement, Industry Users manually enter the following: Name, Social Security Number (SSN), date of birth (DOB), home phone number, email address, driver's license number and state, driver's license address, current street address, and years at the address, which are sent encrypted through the website (https://dcs.faa.gov/) to Equifax Credit Services.[16] PII is sent directly to Equifax via encrypted channel and is not stored or viewed in FAA servers.

Once information is submitted, industry users are required to enter their credit card number, CVC code, expiration year/month, name, billing address and whether the card is issued in the United States, in order to purchase the digital certificate. This data is

[16] Leidos has a Purchase Order with Equifax for purchase of the license.

directly sent encrypted through the website (https://dcs.faa.gov/Certificate/NewCertPayment/) to Elavon Inc. (virtual merchant) who provides the service to purchase digital certificates.[17] In return, Elavon, Inc.[18] sends to the FAA for storage in the WebOPSS database: name, email address, last 4 digits of the credit card number, and a transaction ID number that Elavon auto-generated to track the payment.

Additionally, Industry Users have the option to complete the authentication process offline (this option is mandatory for non-U.S. residents and U.S. residents that have an Identity Protection Service, such as LifeLock). In this case, Industry Users should complete and print a *Proof of Identity Form*[19], notarize it and mail it to Leidos Corporation (this Form does not include a privacy or PRA statement). Leidos does not perform any additional identity proofing and Leidos does not return any of the PII on this form to the FAA. Forms are maintained in a locked file cabinet. Since the inception of the Task Order, no documents have been destroyed. Leidos is currently preparing a Task Order revision to identify a retention period that is consistent with FAA. Leidos uses the PII provided only for identity verification purposes.

Once the notarized form is processed, Industry Users will receive an email notifying them that their Proof of Identity Form was successfully processed including a link to complete the purchase of the digital certificate following the previously described process.

As soon as the credit transaction is approved, the digital certification request is directly sent to GlobalSign.[20] DCS Administrators do not have to manually request the digital certificate through DCS. The process for notification, retrieval, and download of the digital certificate is the same explained for the FAA Users.

OAPS application

Once an Industry User has been approved for certification, they may apply for a small subset of amendments to their operations or management specifications (OpSpecs, MSpecs) related to navigation equipment and procedures using OAPS.

To receive an OAPS account, Industry Users send a request to their Principal Operations Inspector for approval. The Principal Inspector sends a request for an OAPS account approval to the FAA

[17] If individuals have questions about their payment or if a refund is needed, users contact the FAA for Tier 3 support. If there is a credit card issue, individuals will contact Elavon directly. Leidos has no contractual relationship with Elavon.
[18] See Elavon Privacy Policy - https://www.elavon.com/privacy-pledge.html
[19] PII and documents required in the *Proof of Identity Form* are as follows: name, address, company name (optional), email address, telephone number, signature, and a copy of a Government-Issued Photo Identification (Passport or Driver's License). The form also includes PII referred to the certifier: name of the Notary Public / Solicitor / Attorney, country, certification purpose and date, signature, and seal. None of this information is disclosed or communicated to the FAA**,** or to Equifax.
[20] Leidos has a Purchase Order with Global Sign for the purchase of the license.

MyIT Help, and a ticket will be created via the MyITSM Ticketing System. The Principal Inspector sends a request for an OAPS account approval to the FAA MyIT Help Desk via email (helpdesk@faa.gov) in order to add the Industry User to the OAPS user table. The FAA MyIT Help Desk receives the following PII: name, business email address, which organization the user should have access, role, business telephone number.

Once the account is created, the applicant receives an email containing a temporary password with instructions to log in and change the temporary password. Industry Users manage their account through the External User Provisioning (EUP) system, which is another portal (https://avsportal.faa.gov/index.asp) used to reset and manage their account. This portal is outside WebOPSS boundaries[21].

Industry Users are assigned the user category of "Operator", their privileges are limited to submit changes to their operations approvals through the system and to participate in the approval process (e.g. edit, review, print), as required by FAA Users. In order to submit an application, Industry Users select the template to use as a base for the new application and enter the following PII: business contact information, designator code, aircraft registration number, certificate number and operator Identification. In addition, the application includes a checklist tab that displays a list of supporting documents that might be required for some applications and an upload area that Industry Users may use to attach the files to the application. These documents do not provide additional PII and include e.g. training manuals, maintenance procedures, operating procedures and practices. Users are apprised of the appropriate documents to submit via the User Guide and document checklist. There is also a "comments" tab that is a free text field. The comments tab is meant for the user to supply additional information.[22] When the application is submitted, an Application ID number is generated, comprised of a unique string of numbers identifying the application draft.

Once submitted, the FAA User receives an email notification that a task has been created for them in OAPS. Then he or she will review it for completeness and correctness. If the application is not complete and/or correct, the FAA User may return the application to the Industry User for more information, with instructions to resubmit the application. If this happens, the Industry User receives an email message that the application has been returned and may then resubmit the application after the correction is made. The FAA User can also transfer the application to another FAA User or deny it. Both users can add comments during the application lifecycle. If the application is complete and correct, the FAA User can approve the application. THEN WHAT

OPSS Insurance HQ application

OPSS Insurance HQ is part of the certification process for obtaining OpSpecs. During the last phase of the certification, process (Final Certification) the FAA must verify that air carriers have obtained the appropriate liability insurance coverage.

[21] This portal is part of the FAA DS.
[22] There is not currently a warning banner to prevent the user from submitting additional PII. The System Owner has been advised that the System Administrators should redact unnecessary PII.

In order to prove that air carriers have the proper certificate of insurance they are required to complete the following forms and submit them in paper form to the DOT or the FAA, where appropriate:

- Office of the secretary of Transportation (OST) Form 6410 US[23] Carriers Certificate of Insurance
- OST Form 6411 Foreign Air Carriers Certificate of Insurance[24]
- OST Form 4507 Air Taxi Operator Registration and Amendments[25]

OST Forms 6410/6411/4507 must be manually completed (using the PDF Forms), and then printed, and signed. The original signed form must be mailed along with the filing fee (OST Form 4507 only) to the FAA.

- OST Form 6410 or OST Form 6411 include the following PII: Name of the insurer, contact person (name), address, telephone and fax number; name of broker (if applicable), authorized representative (name), address, telephone and fax number. Organization name (air carrier), address, FAA certificate number of insured, effective date. Details of the policy e.g. policy number, type, effective date, amount coverage, aircraft make and model, FAA, foreign flag registration number.

- OST Form 4507 contain the following PII: name of registering carrier, address, telephone number, fax number, and email address, name of authorized representative. Other information such as type of service the carrier intends to perform, aircraft make and model, FAA registration number, passenger seats.

Once these forms are received by the FAA, FAA Users enter the information manually into the OPSS Insurance HQ application.

The Insurance HQ application will be replaced by the Economic Authority and Insurance Management (eAIM) system, which is currently under development[26]. eAIM will transfer and maintain all of the data from the current OPSS Insurance HQ application for use in the new system. It will allow direct online submission to the FAA by the responsible parties of OST Forms 4507, 6410 and 6411. It will capture OST form information directly as entered without

[23] OST Form 6410, OMB 2106-0030, Expiration 02/28/2011, includes a Paper Reduction Act Notice, but not a privacy notice. This form is expired. This form is managed by DOT/OST and is outside FAA's boundaries. OST program office has started the process of reinstatement of Information Collection Request with OMB Control number 2106-0030 2017 and should be completed not later than November 30th.
[24] OST Form 6411, OMB 2106-0030, Expiration 09/30/2007, includes a Paper Reduction Act Notice, but not a privacy notice. This form is expired (see previous Footnote).
[25] OST Form 4507, OBM 2105-0565, Expiration 06/30/2019, includes a Paper Reduction Act Notice. This form is managed by DOT/OST and is outside FAA's boundaries.
[26] This application is part of the FY17 assessment, but is scheduled to be implemented on or about the end of FY18.

requiring Insurance Analysts to enter the information provided on the forms. eAIM will send notifications to the appropriate Insurance Analyst(s) or department when applicants submit forms. It will send notifications to the Principal Operations Inspector (POI) for the operator when an operator or insurance company submits a form. It will provide economic authority status and information to WebOPSS for display within WebOPSS Certificate Holding District Office (CHDO) and will expand the use of "Insurance in a Non-Compliant State" notification regarding economic authority and insurance status displayed in WebOPSS. The application is expected to process the same PII as the OPSS Insurance HQ application. The application is still in development.

OPSS Exemptions HQ application

During the last phase of the certification process, Industry Users are required to list all exemptions and deviations in their OpSpecs[27]. OPSS Exemption HQ facilitates the process of listing grants of exemptions obtained in the OpSpecs.

Petitions for exemption are submitted by Industry Users electronically to the Federal Docket Management System (FDMS) or in writing to the Docket Management Facility US Department of Transportation. Once received into FDMS, the FAA Office of Rulemaking processes the petition for exemption and renders a decision, which is also published through the Automated Exemptions System (aes.faa.gov) in a letter format addressed to the petitioner by name, title, organization and mailing address. The exemption petition and review process are outside the scope of WebOPSS/OPSS Exemptions HQ[28].

FAA employees enter the information for Grants of Exemption published manually into the OPSS Exemption HQ component. PII entered into the application includes petitioner's name, organization, address, and role/title. PII on FAA Users contained in OPSS Exemption HQ includes their name, role/title, FAA office, and username.

OPSS Exemption HQ also provides search options for specific exemption entries in order to review their status, or filter out certain types of entries in order to reduce the number to be displayed. Other functionalities include add, edit or delete entries from the list of exemption petitioners for use when assigning exemptions to certificate holders, load the exemption (a word document) from the workstation to the application and download copies of the exemptions.

Data Exchanges

See Section 2.10 for a description of data exchanges.

Reports

[27] 14 CFR Part 119, Section 119.49
[28] This process is outside WebOPSS' boundaries, it is part of another system: Integrated Rulemaking Information Management System (IRMIS). IRMIS has an adjudicated PTA, dated September 29, 2015.

WebOPSS contains audit logs which could include username. The DCS application audit logs also include: name, email address (of Industry Users and FAA Users), and the last 4 digits of the credit card number used in the transaction (Industry Users only). Reports can also be developed in the applications, such as reports of individuals who have been issued digital certificates (in DCS) and Application Status Reports by Region (OAPS). PII that could be present in these reports includes any of the PII maintained in the WebOPSS database.

2 INFORMATION MANGEMENT

2.1 SUBJECTS of Collection

Identify the subject population(s) for whom the system collects, maintains, or disseminates PII. (Check all that apply)

☒ **Members of the public:**

☒ **Citizens or Legal Permanent Residents (LPR)**

☒ **Visitors**

☒ **Members of the DOT Federal workforce**

☒ **Members of the DOT Contract workforce**

☐ **System Does Not Collect PII.** If the system does not collect PII, proceed directly to question 2.3.

2.2 What INFORMATION ABOUT INDIVIDUALS will be collected, used, retained, or generated?

Subsystem	FAA employees/contractors	Members of the public (air operators and air agencies)
WebOPSS	• Name • Role/title • Organization • FAA email address • Telephone number • Office code/location • Address • Username	• Name • Role/title • Organization • Address • Email address • Telephone number • Username • Aircraft registration number • Certificate number/status/type
DCS	• Name • FAA email address • Office • Location • Certificate ID number • Certificate expiration date • Username	• Name • Email address • Company • Certificate ID number • Certificate expiration date • Last 4 digits of credit card used to purchase

		• Amount and date of purchase • Transaction ID • Credit card number (not maintained in DCS database) • SSN (not maintained in DCS database) (DCS only – users have the option to use Leidos Proof of Identity form instead) • DOB (not maintained in DCS database) • home phone number (not maintained in DCS database) • driver's license number and state(not maintained in DCS database) • driver's license address, current street address, and years at the address(not maintained in DCS database) • Photocopy of government issued photo identification (Leidos Proof of Identity Form only. Not stored in DCS database)
OAPS	• Name • Role/title • Organization • FAA email address • Telephone number or cell number (optional) • Office code/location • Address • Username	• Name • Role/title • Organization • Address • Email address • Telephone number • Username • Designator code • Certificate number • Operator ID • Aircraft registration number • Application ID
OPSS Insurance HQ	• Name • Role/Title • Telephone number • Fax • Address • Username	• Name of the insurer • Contact person (name) • Address • Telephone number • Fax number • Name of the broker (if applicable) • Authorized representative (name) • Address • Telephone number • Fax number • Foreign flag registration number • Organization name (air carrier) • FAA certificate number of insured

OPSS Exemptions HQ	• Name • Role/title • Office • Username	• Name • Role/Title • Organization • Address

2.3 Does the system RELATE to or provide information about individuals?

☒ **Yes**:

The WebOPSS system contains PII on the FAA employee/contractor workforce who are users of the system including within audit logs. The system also contains information from members of the public who represent air operators and air agencies and who submit operations specifications applications on their behalf.

☐ **No**

If the answer to 2.1 is "*System Does Not Collect PII*" **and** the answer to 2.3 is "*No*", you may proceed to question 2.10.
If the system collects PII or relate to individual in any way, proceed to question 2.4.

2.4 Does the system use or collect SOCIAL SECURITY NUMBERS (SSNs)? (This includes truncated SSNs)

☒ **Yes:**

Authority:

]

Purpose:
Industry users who are requesting digital certificates provide their SSNs on a web transmittal page that forwards their SSN directly to Equifax. SSN is not maintained in the DCS database. The purpose of the collection of SSN is used for identity verification.

In order for the Federal Government to identify, verify and authenticate an external user from the public, the National Institute of Standards and Technology (NIST) Special Publication 800-63-2, "Electronic Authentication Guidelines," requires that the federal government collect and use an individual's information located on a government-issued identification document for that individual. In particular, the SSN is used to cross-reference an individual with additional data elements using an identity verification tool or

service, such as Equifax. The data elements in this case are provided collected directly by Equifax for identity-proofing, and not by the FAA, and are not stored in any FAA system.

The disclosure of the SSN is voluntary in this case, as there is another option for identity proofing available. Individuals can provide a notarized form to Leidos that does not require the individual's SSN. The DCS website informs the individuals of the option to provide the notarized Leidos form – although they have been advised that they need to make it clear that this is an alternative to providing the SSN to Equifax.

☐ **No**: The system does not use or collect SSNs, including truncated SSNs. Proceed to 2.6.

2.5 Has an SSN REDUCTION plan been established for the system?

☐ **Yes:**

☒ **No:** While DCS has a transmittal page where users input SSN, SSN is not stored in the DCS database.

2.6 Does the system collect PSEUDO-SSNs?

☐ **Yes:**

☒ **No**: The system does not collect pseudo-SSNs, including truncated SSNs.

2.7 Will information about individuals be retrieved or accessed by a UNIQUE IDENTIFIER associated with or assigned to an individual?

☒ **Yes**

Is there an existing Privacy Act System of Records notice (SORN) for the records retrieved or accessed by a unique identifier?

☒ **Yes:**

SORN:

- DOT/ALL 9, Identification Media Record Systems, October 7, 2002 67 FR 62511
- DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002 67 FR 30757
- DOT/FAA 847, Aviation Records on Individuals, November 9, 2010 75 FR 68849.

DOT/ALL 13

DOT/FAA 847

☐ **No:**

Explanation:

Expected Publication:

☐ **Not Applicable:** Proceed to question 2.9

2.8 Has a Privacy Act EXEMPTION RULE been published in support of any Exemptions claimed in the SORN?

☒ **Yes**

Exemption Rule:

DOT/FAA 847, Aviation Records on Individuals, November 9, 2010 75 FR 3058. Records in this system that relate to administrative actions and legal enforcement actions are excepted from certain access and disclosure requirements of the Privacy Act of 1974, pursuant to 5 U.S.C. 552a(k)(2).

☐ **No**

Explanation:

Expected Publication:

☐ **Not Applicable**: SORN does not claim Privacy Act exemptions.

2.9 Has a PRIVACY IMPACT ASSESSMENT (PIA) been published for this system?

☐ **Yes:**

☒ **No**:

☐ **Not Applicable:** The most recently adjudicated PTA indicated no PIA was required for this system.

2.10 Does the system EXCHANGE (receive and/or send) DATA from another <u>INTERNAL</u> (DOT) or <u>EXTERNAL</u> (non-DOT) system or business activity?

☒ **Yes:**

<u>Internal Data Exchanges:</u> WebOPSS does not currently have PII Data Sharing Agreements for its internal data exchanges. The System Owner has been advised to reach out to the PII Data Sharing Agreement POC for assistance.

- **FAAMIS** – Provides a system record of information about certified entities (e.g. air carriers and air operators), aircrafts and airmen. WebOPSS sends data to FAAMIS on a two-way connection via TCP over SQL, including the following PII: name of Industry Users' personnel, title, address, name of the FAA principal inspector in the certificate. SORN coverage for FAAMIS has not yet been determined, as FAAMIS does not yet have an adjudicated PTA.
- **SPAS** – SPAS consolidates information from different flight standards. WebOPSS sends data to SPAS on a one-way connection via TCP over SQL

including all PII data within the WebOPSS database. SORN coverage for SPAS has not yet been determined, as SPAS does not have an adjudicated PTA.

- **CETS** – CETS supports a drug enforcement program. WebOPSS sends data via TCP over SQL to SPAS on a one-way connection including all PII data within the WebOPSS database. SORN coverage is via DOT/FAA 847.
- **VDRP** – VDRP supports a voluntary data reporting program. WebOPSS sends data via TCP over SQL to VDRP on a one-way connection including all data in the WebOPSS database. VDRP does not retrieve information by personal identifier and so is not covered by a SORN.
- **SAS** – SAS provides support to FAA safety programs and risk management processes. WebOPSS sends data to VDRP via TCP over SQL on a one-way connection including the following PII: name of Industry Users' personnel, title, address, name of the FAA principal inspector in the certificate. The records are covered under: DOT/FAA 801 and DOT/FAA 847.
- **FAA DS –** FAA DS is used to authenticate users in WebOPSS, using AD. WebOPSS only receives an access token, which is generated by AD and sent encrypted to WebOPSS, once the user credentials have been verified. SORN coverage is via DOT/ALL 13.
- **MyITSM –** MyITSM receives via email exchange account requests. PII received from WebOPSS users includes: name, role/title, organization, FAA email address, telephone number, office code/location, office address and access privileges. SORN coverage is via DOT/ALL 13.

External Data Exchanges:

The FAA does not currently have Memorandums of Understanding (MOU) with these entities. FAA has a Task Order with Leidos. Leidos has Purchase Orders with GlobalSign and Equifax for purchase of licenses.

- **Elavon, Inc.** – the FAA DCS webpage acts as a transmittal page (name, email address, credit card number, expiration date, security code) to send payment information to Elavon, avoiding the WebOPSS database. However, Elavon does send to WebOPSS a transaction ID, name email address and the last 4 digits of the user's credit card number to WebOPSS for storage in the WebOPSS database.
- **GlobalSign -** Once DCS Administrators receive the digital certificate request; they will be authorized to generate the digital certificate by navigating to the site https://dcs.faa.gov/ and using their Administrator credentials (username and password). Once in the system, DCS Administrators manually enter the following PII of the individual needing a certificate: name, FAA email address, office, and location. This information is transferred to GlobalSign. Once the signature process is initiated, industry users will receive two automated emails. Once email

has detailed instructions regarding the user's retrieval password. The second email will include a certificate ID and link to download.

- **Equifax –** Industry Users are required to manually provide the following: Name, SSN, DOB, home phone number, email address, driver's license number and state, driver's license address, current street address, and years at the address, which are directly sent encrypted through the website (https://dcs.faa.gov/) to Equifax Credit Services. The information exchange is private and only between Industry Users and Equifax Inc. PII is sent directly to Equifax via encrypted channel and is not stored or viewed in FAA servers. Equifax sends the DCS application a pass/fail rating and reason code.
- **Leidos –** Industry users may complete and print a *Proof of Identity Form*[29], notarize it and mail it to Leidos Corporation (this Form does not include a privacy statement) – Through this process Leidos Inc. verifies Industry User's identity. Leidos does not return any of the PII on this form (which includes: name, address, company name, email, phone number, signature, copy of government issued photo identification) to the FAA. Forms are maintained in a locked file cabinet. Since the inception of the Task Order, no documents have been destroyed. Leidos is currently preparing a Task Order revision to identify a retention period that is consistent with FAA. Leidos uses the PII provided only for identity verification purposes.

☐ **No**

2.11 Does the system have a National Archives and Records Administration (NARA)-approved RECORDS DISPOSITION schedule for system records?

☒ **Yes:**

Schedule Identifier:

NCI-237-77-03 Items 31 & 33 – Proposed Big Bucket Schedule which will supersede these schedules is DAA-237-2016-0012-0015

II-NNA-1102 items 17 & 19 – Proposed Big Bucket Schedule which will supersede these schedules is DAA-0237-2016-0012-0061

[29] PII and documents required in the *Proof of Identity Form* are as follows: name, address, company name (optional), email address, telephone number, signature, and a copy of a Government-Issued Photo Identification (Passport or Driver's License). The form also includes PII referred to the certifier: name of the Notary Public / Solicitor / Attorney, country, certification purpose and date, signature, and seal. None of this information is disclosed or communicated to the FAA.

nc1-237-77-03.pdf

ii-nna-001102_sf115.pdf

Schedule Summary:

NCI-237-77-03

Item 31: Air Carrier Maintenance Files

(a) Regional Flight Standards Offices – Destroy when 10 years old, except that basic certificates, specifications, and authorizations are to be destroyed eight years after being superseded or canceled. Transfer to Federal Records Center after 5 years, except that basic certificates, specifications, and authorizations are to be transferred 5 years after being superseded or canceled.

(b) Flight Standards field offices – Destroy after 5 years, except that basic certificates, specifications, and authorizations are to be destroyed 5 years after being superseded or canceled.

Item 33: Air carrier operations files

(a) Regional flight standards offices – destroy after 10 years, except that basic certificates, specifications and authorizations are to be destroyed 8 years after being superseded or canceled. Transfer to Federal Records Center after 5 years, except that basic certificates, specifications and authorizations are to be transferred 5 years after being superseded or canceled.

II-NNA-1102 items 17 & 19

Item 17: Approved Schools Case Files

(a) Maintain 2 sets of files 1) currently active file of active schools; and 2) semi-active files of inactive or cancelled schools

(b) When a specific inactive or canceled school is recertified, remove folder from inactive or cancelled file and return folder to the active file.

(c) Screen inactive files annually and destroy all files which have been inactive for 5 years.

Item 19: "Air Taxi" Case Files

(a) Basic certificates and data to be destroyed 3 years after superseded or cancelled.
(b) All other records to be destroyed when 3 years old.

☐ **In Progress**

☐ **No:**

3 SYSTEM LIFECYCLE

The systems development life cycle (SDLC) is a process for planning, creating, testing, and deploying an information system. Privacy risk can change depending on where a system is in its lifecycle.

3.1 Was this system IN PLACE in an ELECTRONIC FORMAT prior to 2002?

The E-Government Act of 2002 (EGov) establishes criteria for the types of systems that require additional privacy considerations. It applies to systems established in 2002 or later, or existing systems that were modified after 2002.

☒ **Yes**: 1/1/1998

☐**Not Applicable**: System is not currently an electronic system. Proceed to Section 4.

3.2 Has the system been MODIFIED in any way since 2002?

☒ **Yes**: The system has been modified since 2002.

☒ **Maintenance.**

☒ **Security.**

☒ **Changes Creating Privacy Risk**:

Since the date of the FAA-reviewed PTA, WebOPSS has undergone significant changes; including major functionality changes for the DCS component, leading to the addition of significant additional PII, including SSNs, among other PII data elements. The previous PTA did not include any data sharing; this PTA is updated to describe the data sharing with internal and external systems.

☐ **Other**:

☐ **No**: The system has not been modified in any way since 2002.

3.3 Is the system a CONTRACTOR-owned or -managed system?

☐ **Yes**: The system is owned or managed under contract.

Contract Number:

Contractor:

☒ **No**: The system is owned and managed by Federal employees.

3.4 Has a system Security Risk CATEGORIZATION been completed?

The DOT Privacy Risk Management policy requires that all PII be protected using controls consistent with Federal Information Processing Standard Publication 199 (FIPS 199) moderate confidentiality standards. The OA Privacy Officer should be engaged in the risk determination process and take data types into account.

☒ **Yes**: A risk categorization has been completed.

Based on the risk level definitions and classifications provided above, indicate the information categorization determinations for each of the following:

Confidentiality:	☐ Low	☒ Moderate	☐ High	☐ Undefined
Integrity:	☐ Low	☒ Moderate	☐ High	☐ Undefined
Availability:	☐ Low	☐ Moderate	☒ High	☐ Undefined

Based on the risk level definitions and classifications provided above, indicate the information system categorization determinations for each of the following:

Confidentiality:	☐ Low	☒ Moderate	☐ High	☐ Undefined
Integrity:	☐ Low	☒ Moderate	☐ High	☐ Undefined
Availability:	☐ Low	☐ Moderate	☒ High	☐ Undefined

☐ **No:** A risk categorization has not been completed. Provide date of anticipated completion.

3.5 Has the system been issued an AUTHORITY TO OPERATE?

☒ **Yes:**

Date of Initial Authority to Operate (ATO): 09/29/2017

Anticipated Date of Updated ATO: 09/29/2020

☐ **No:**

☐ **Not Applicable**: System is not covered by the Federal Information Security Act (FISMA).

4 COMPONENT PRIVACY OFFICER ANALYSIS

The Component Privacy Officer (PO) is responsible for ensuring that the PTA is as complete and accurate as possible before submitting to the DOT Privacy Office for review and adjudication.

COMPONENT PRIVACY OFFICER CONTACT Information

Name: Bud Gordon

Email: bud.gordon@faa.gov

Phone Number: 571-209-3078

COMPONENT PRIVACY OFFICER Analysis

I have reviewed the AVS WebOPSS PTA and found the risk level as High as reflected in the risk categorization in the PTA.

WebOPSS consists of a suite of five applications that allow for the certification and authorization for air operators and air agencies to conduct business and fly in the national airspace.

Since the date of the previously reviewed PTA, the WebOPSS system has undergone significant changes, including major functionality changes for the DCS component and the addition of significant additional PII including SSNs, among other PII data elements. The previous PTA did not include any data sharing; this PTA is updated to describe the data sharing with internal and external systems. The system acts as a pass thru for SSNs to Equifax. The FAA SSN Reduction POC responded that "since SSNs are not stored in the system it would not require further action for the SSN Reduction Plan."

I have reviewed the WebOPSS PTA and found the risk level as moderate as reflected in the PTA. The WebOPSS system is a privacy system based upon the data elements it collects, I recommend the SORNs to be DOT/ALL 13, DOT/ALL 9, and DOT/FAA 847 as reflected in the PTA. The previous PTA was drafted but not adjudicated. The data disposition schedules are NCI-237-77-03 Items 31 & 33 and II-NNA-1102 items 17 & 19.

5 COMPONENT REVIEW

Prior to submitting the PTA for adjudication, it is critical that the oversight offices within the Component have reviewed the PTA for completeness, comprehension and accuracy.

Component Reviewer	Name	Review Date
Business Owner	Jean Mortellaro	5/10/2018
General Counsel	Sarah Leavitt	9/18/2018
Information System Security Manager (ISSM)	None	None
Privacy Officer	Bud Gordon	9/18/2018

Records Officer	Kelly Batherwich	3/15/18

Table 1 - Individuals who have reviewed the PTA and attest to its completeness, comprehension and accuracy.

TO BE COMPLETED BY THE DOT PRIVACY OFFICE

Adjudication Review COMPLETED: September 26, 2018

DOT Privacy Office REVIEWER: Claire W. Barrett

DESIGNATION

☐ **This is NOT a Privacy Sensitive System – the system contains no Personally Identifiable Information.**

☒ **This IS a Privacy Sensitive System**

- ☐ **Category of System**
- ☐ **IT System.**
- ☐ **National Security System.**
- ☐ **Legacy System.**
- ☐ **HR System.**
- ☐ **Rule.**
- ☒ **Other:**

DETERMINATION

☐ ***PTA is sufficient at this time.***

☐ ***Privacy compliance documentation determination in progress.***

PIA

☐ ***PIA is not required at this time:*** *<<Rationale>>*

☒ ***PIA is required.***

- ☐ ***System covered by existing PIA:*** *<<Identify PIA>>*
- ☒ ***New PIA is required.*** collects sensitive PII from members of public.
- ☐ ***PIA update is required.***

SORN

☐ ***SORN not required at this time.*** *<<Rationale>>*

☒ ***SORN is required.***

- ☒ **System covered by existing SORN:** see adjudication statement
- ☐ ***New SORN is required.*** see adjudication statement
- ☐ ***SORN update is required.*** see adjudication statement

Departmental Chief Privacy Officer (CPO) Adjudication Statement

DOT CPO has determined that RPFMT is a privacy sensitive system.

POA&M

- *AR-2(b)- Privacy Impact and Risk Assessment/PIA*

  Issue: System collects PII from members of the public; data elements and or system create significant privacy risk to individuals. Requirement: Provide updated PIA to DOT CPO. Timeline: 90 days.

- *AP-1 – Authority to collect. IP-1(a-b) Consent/Consent/Consequences*

  Issue: FAA has not identified authority authorizing mandatory collection of SSN and the system does not include appropriate Privacy Act notice providing individual information on the voluntary nature of SSN collection, consent for its use, and consequences for failure to provide. Requirement: Implement appropriate Privacy Act notice and mechanism for consent. Timeline: 30 days.

- *DM-1(a-c) - Minimization of Personally Identifiable Information/Limited Collection, Relevant & Necessary*

  Issue: FAA has not established clear need or authority to maintain SSN in the environment. Requirement: Establish and implement system specific plan to remove unnecessary SSN from the environment. Provide plan to DOT CPO. Timeline: 120 days. NOTE: The general SSN management plan does not fulfill this requirement.

- *DM-2(a-c) Data Retention and Disposal/Retention/Scheduling/Secure Destruction; SI-12 – Information Handling and Retention*
  Issue: Referenced records schedule does not match FAA declaration that records are about individuals (see SORN) nor does it match the state purpose of the system Therefore the FAA cannot be appropriately implementing its records management responsibilities. Requirement: Establish file plan for system and as necessary develop/update records disposition schedule. Provide File Plan and Disposition Schedule to DOT CPO and DOT Records Officer. Timeline: 90 days.

- *IP-1(a) Consent/Consent; TR-1(a-b) Privacy Notice/Notice/Purpose*
  System access does not have appropriate Privacy Act notices informing individuals that their records will be maintained under DOT/FAA 847. Requirement: Implement appropriate Privacy Act notices on all collection instruments including but not limited to website associated with system. Timeline: 90 days NOTE: Notice must be consistent with SORN analysis.

- *TR-2(a) – System of Records Notices and Privacy Act Statements; AP-1 Authority to Collect*
  Issue: Reference SORN does not match system description or referenced records schedules. Records in the system do no appear to be about an individual, rather that they are about aircraft. Requirement: Conduct comprehensive system and business process

review to determine applicability of Privacy Act to records. Provide review outcomes to DOT CPO. Timeline: 90 days

- *SE-1(a) - Inventory of Personally Identifiable Information/System Inventory* Issue: System maintains SSN. Requirement: Update CSAM record to reflect SSN holdings. Timeline: 30-days from issuance of DOT Guidance for updating CSAM record.

NOTE: In its 2014 and 2017 Quality Control Review of Controls Over DOT's Protection of Privacy Information the DOT Inspector General noted that Departmental IT systems need to improve "ongoing validation of specific privacy related security controls for their systems are in effect, including those that safeguard confidentiality, provide secure remote access, encryption of back up media, follow up of unauthorized mobile devices, and proper user account and password settings in accordance with DOT policy. " FAA management is strongly encouraged to review NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) and make an active determination regarding the applicability of the specific security controls identified in section 4.3 of the same.

NOTE: Records about users of the system are collected for the purposes of creating and maintaining accounts. These records are protected under the Privacy Act and must be maintained in accordance with DOT/ALL 13 - Internet/Intranet Activity and Access Records - 67 FR 30757 - May 7, 2002.

The Adjudicated PTA should be uploaded into CSAM as evidence that the required privacy analysis for this system has been completed.

The PTA should be updated not later than the next security certification and accreditation (C&A) cycle and must be approved by the DOT PO prior to the accreditation decision. Component policy or substantive changes to the system may require that the PTA be updated prior to the next C&A cycle.