Privacy Threshold Assessment (PTA)

Federal Aviation Administration (FAA)
Office of Aviation Safety (AVS)
Simulator Inventory & Evaluation Scheduling System (SIESS)

CLAIRE W BARRETT Digitally signed by CLAIRE W BARRETT
Date: 2018.11.20 13:03:49 -05'00'

11/20/2018

X Claire W. Barrett

Claire W. Barrett
DOT Chief Privacy Officer
Signed by: CLAIRE W BARRETT

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: Simulator Inventory & Evaluation Scheduling System (SIESS)

Cyber Security Assessment and Management (CSAM) ID: 1420

SYSTEM MANAGER CONTACT Information:

Name: Craig Merrill

Email: craig.merrill@faa.gov

Phone Number: (501) 918-4444

Is this a NEW system?

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

Is there a PREVIOUSLY ADJUDICTED PTA for this system?

☒ **Yes:**

Date: 1/22/2014

☐ **No**

1 SUMMARY INFORMATION

1.1 System TYPE

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

Unique Investment Identifier (UII): 021-615337796

Cyber Security Assessment and Management (CSAM) ID: 1420

☐ **Paper Based:**

☐ **Rulemaking**

Rulemaking Identification Number (RIN):

Rulemaking Stage:

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

Federal Register (FR) Notice:

☐ **Information Collection Request** (ICR)[3]
- ☐ **New Collection**
- ☐ **Approved Collection or Collection Renewal**
  - ☐ **OMB Control Number:**
  - ☐ **Control Number Expiration Date:**

☐ **Other:**

1.2 System OVERVIEW:

The Federal Aviation Administration (FAA) is updating the Simulator Inventory & Evaluation Scheduling System (SIESS) Privacy Threshold Analysis (PTA) that was previously-adjudicated on 1/22/2014. Since the date of adjudication of the PTA, SIESS' data exchange with the Air Transportation Oversight System (ATOS) has discontinued as the ATOS system was decommissioned[4]. In addition, SIESS has been scheduled to convert to a completely web-based application. This transition will require the Personal Computer (PC) aspect of the system to sunset. The web-based SIESS will include several new modules including the Safety Quality Management System (SQMS) which will be used to evaluate and certify the quality management of Flight Training Device (FSTD) operators. Further, it has been determined that all information related to individuals is collected and used only in a business capacity. This applies not only to the existing SIESS functioning, but to the new modifications described.

The Scheduling aspect of the PC-based system is currently not in use but the functionality will be incorporated into the new system. The transition to the web-based SIESS is scheduled to be completed in October or November 2018. SIESS currently only serves as a repository for information on simulators. The security assessment for SIESS was completed at a point in time review of the system; therefore there may be differences in information between the April 2018 System Characterization Document (SCD) and this current PTA which contains more recent information. Additional or new information that does not match the data in the SCD will be addressed during the next security assessment. The security assessment identified a Plan of Action and Milestone (POAM) for SIESS that also presents a privacy risk for the PII in the system: SIESS does not protect the confidentiality and integrity of information in transit through cryptographic mechanisms. In addition, SIESS does not encrypt data at rest. Encrypting data in transit and at rest will minimize loss of data due to theft or unauthorized access or other malicious activities. The POAM notes that the System Owner plans to address this risk in the upcoming SIESS conversion to a web-based application.

The SIESS supports the Office of Aviation Safety (AVS) National Simulator Program (NSP) in qualifying all simulators used to train pilots who operate in United States airspace. The upgraded SIESS will be used to schedule evaluations of these devices and act as a repository

[3]See 44 USC 3201-3521; 5 CFR Part 1320
[4] The ATOS System Disposal Assessment (SDA) was adjudicated by the DOT Chief Privacy Officer (CPO) on 11/4/2016.

of information on simulators (e.g. site location, sponsor, manufacturer). Currently, the system is used solely as a repository for information and evaluations on simulators. Simulator evaluation scheduling is now carried out manually by NSP staff and scheduling information is not entered into the system. The system is hosted at the FAA Enterprise Data Center at the Mike Monroney Aeronautical Center, 6500 South Macarthur Boulevard, Oklahoma City, Oklahoma 73169-6901.

SIESS is used only by FAA employees, specifically a limited number of AVS inspectors and selected NSP staff including the simulator evaluation scheduling staffer. AVS inspectors previously used the system to schedule simulator evaluations and check the status of simulators. The new system will return that functionality. NSP staff use SIESS to maintain information on simulators. A Uniform Resource Locator (URL) for the proposed web-based system has not yet been established. System users are authenticated by Personal Identity Verification (PIV).[5] Users request access by contacting the MyIT Help Desk.[6]

Once users have been approved to access SIESS by the AFS-205 Manager, the MyIT Help Desk adds them to the AFS2050Grp_Staff; the program is installed on their AVS Workstation; and they are then able to use the shared SIESS PC application. Users are authenticated to SIESS through their FAA Domain ID/Active Directory[7] account used to log on to their workstation. The application is PIV-enabled, via Integrated Windows Authentication (IWA).

SIESS is currently and will continue to be used primarily as an authoritative source of information on simulators and FSTDs[8] as well as the business contact information for simulator sponsoring organizations in the United States. Information on FSTDs is manually updated within the system as it is submitted to the NSP program office. The SIESS homepage provides links for the following functions: Simulators, FTDs[9], Data Maintenance, Schedule, Reports, Program Management, and Administration. The Simulators function allows users to access information on simulators, define new simulators, and edit existing information on simulators. The FTDs function allows users to define new FSTDs and edit FSTDs. The Data Maintenance function allows users to edit information on simulators such as company, personnel, and aircraft information. The Schedule function is no longer in operation. Previously, it allowed users to schedule simulator evaluations. The Reports function allows users to view and print reports regarding simulator scheduling, checklists, and personnel. The Program Management function allows users to manage program manager assignments and review evaluations. The Administration function provides for administrative activities such as data uploads of simulator information. Currently, an NSP staff member

[5] PIV information such as PIV card serial number does not traverse the system boundary and is not stored in the system.
[6] The MyIT Help Desk New User Form includes the following PII: First Name, Middle Initial, Last Name, Contractor Firm, Address, Position Series/Title, Email Address, User ID. The New User Form is submitted directly

to the MyIT Help Desk. The information on the form is not entered into SIESS.
[7] The FAA Directory Services ("AIT Directory Services") PTA adjudication is pending at DOT.
[8] FSTD is the broad term for devices used for flight training (e.g. a magnetic board with symbols used for training). Simulators are a type of FSTD.
[9] The SIESS homepage lists “FTDs” however this is a typographical error, the correct term is FSTD.

manages the schedule for simulator evaluations offline and notifies stakeholders, investigators, and staff when an evaluation is pending or past due.

The SIESS upgrade will contain the following modules:

- Company
- FSTD
- Evaluation
- DR (DR, MMI, NQT)
- Modification
- SQMS
- Scheduling
- Alert (Action Item 'To-Do' List)
- Query/Report – Reporting function
- Correspondence, Documentation, Forms – templates for NSP forms
- PM (Program Management)

None of these modules will collect any more PII than is already being collected in the current SIESS platform.

The Company module will be used to create new records for sponsors and manufacturers and view new/existing sponsors/manufacturers along with specific information, i.e. Name, Type of company, Company ID number, SQMS status, etc.

The FSTD module will be used to create new FSTD records and view new/existing FSTDs along with specific information, i.e. FAA ID number, Sponsor Company, FSTD level, etc (see NSP Form T001A).

The Evaluation module will allow NSP evaluation personnel to review all relevant FSTD data prior to an evaluation event. The module will also facilitate management of the evaluation event to include capture of inspection data on the evaluation report (NSP Form T002), capture of any FSTD modifications since the last evaluation, capture of DR/MMI/NQT items, entry of the next evaluation date, creation of or change to the FSTD configuration sheet (NSP Form T001A), and creation of or change to the Statement of Qualification (SOQ – NSP Form T001). This module will assist the NSP evaluation team with the final evaluation out-briefing to the sponsor at the conclusion of the evaluation by presenting the evaluation products in a format that can be presented or printed.

The DR/MMI/NQT module will be utilized to create FSTD discrepancies, MMI items, and or Non-Qualified Tasks (NQT) typically as a result of FSTD evaluation. The functionality also includes the ability to assign due dates and or update status. It allows authorized personnel to view DR/MMI/NQT information specific to FSTDs and/or Sponsor companies and manage the information through query, filter, etc.

The Modification module will be used to create new data notifications for FSTDs, FSTD modification requests, provide for the review, and disposition by NSP personnel. It also allows for archiving of notifications or modifications in such a way that NSP personnel may see a "history" for each FSTD. It is connected to the Evaluation module in such a way that creation of an FSTD evaluation (when required) is easily accomplished.

The SQMS module will be utilized to create SQMS assessment events and facilitate management of SQMS programs for Sponsor companies. This includes creating records of programs for Sponsor companies, uploading and associating files with those companies, indicating the status of SQMS programs and assessment events, and the capture of audit data on the assessment report (NSP Form T035).

Regarding Alerts, SIESS will display an Action Item "To Do" list on the user home page. Action items will be changes/submissions/actions by external users. SIESS will make action items accessible via a hyperlink which takes the user directly to the record that requires action.

Regarding Queries and Reports, SIESS will be able to produce standard as well as custom AD HOC reports. SQL Server Reporting services will be used for all Query/Report capabilities listed. SIESS will further be able to export all queries/reports into a spreadsheet file.

The Scheduling module will be used to assign dates (or change already assigned dates) to events (FSTD Eval and/or SQMS), assign resources, create event calendars, communicate event to appropriate people via documents and to generally manage the evaluation and assessment operations.

With regard to Correspondence, Documentation, and Forms SIESS shall provide a template for: a Statement of Qualification (NSP Form T001); a Configuration List (NSP Form T001A); an Evaluation Report (NSP Form T002); a Continuing Evaluation Notification Letter (NSP Form T007); an Initial Evaluation Notification Letter (NSP Form T008); a New Data Notification Form (NSP Form T011); a Modification Form (NSP Form T011); a Modification Form (FD2) (NSP Form T011-FD2); an Initial/Upgrade Evaluation Request (NSP Form T025); an SQMS Onsite Assessment Form (NSP Form T035); and a Configuration List (NSP Form T001A). In addition, SIESS will produce the correspondence listed in SIESS Notifications (current version), fill in the case specific data, and automatically update any associated database elements, e.g. dates, types, etc.

SIESS will also contain a PM module that will facilitate the assignment of NSP personnel to act as NSP Program Managers for a group of active FSTDs.

Typically, NSP staff use SIESS to check existing FSTD records or make minor edits to records based on recent evaluations. However, during the infrequent cases when a new simulator must be added to SIESS, NSP staff physically visit the simulator and fill out Form T001A[10] to document the status of the FSTD. Form T001A contains the following PII: name; address, city, state/province/territory, country, zip code, sponsor identification (ID) number (FAA designator)[11], telephone number, email address, office ID, fax number, FSTD ID number, and an open-text area for remarks. After gathering information on the simulator during the site visit, NSP staff return to their home office and manually enter the information on the form into SIESS. SIESS users click the SIESS icon on their workstations to open the

[10] Form T001A

[11] The 'Designator' is the first 4 characters in a user's operator certificate number issued by the FAA.

program. At the homepage, users then click the 'Simulators' button so that they can add a new FSTD record, edit a record, or check information on a record. Users may also enter the simulator ID in the 'Simulator ID' field to choose a record to edit. Users then create the record by inputting the Form T001A data fields.

SIESS contains the following business contact information for points of contact for sponsoring organization including: name, business address, business phone number, sponsor identification (ID) number (FAA designator), email address, office ID, fax number, and FSTD ID number. SIESS also contains information on AVS Inspectors which includes: individual's name, FAA Employment Code and a check box indicating whether the employee is active or not. The contact information record and Simulator records also contain open-text fields for notes and Simulator Owner information, however NSP does not anticipate that additional PII would be added to either field. This information is added to the system manually via a web interface.

SIESS users may also generate FAA Statements of Qualification (SOQ) through an associated URL, https://afs600.avs.faa.gov/siess.[12] SOQ's are certifications from the FAA NSP stating that an FSTD has been evaluated and met qualifications. SOQ's contain the following PII: Full name and signature of the FAA Manager of the NSP.

SIESS exchanges data with the following DOT/FAA systems (see Section 2.10 below for details):

Safety Assurance System (SAS)[13], Safety Performance Analysis System (SPAS)[14] FAA Directory Services ("AIT Directory Services") (see footnote 9), and Federal Aviation Administration Management Information System (FAAMIS).[15]

SIESS contains a Reports function which allows users to choose from the following reporting options: Monthly Status of Evaluations; Monthly Evaluation Schedule; Next Scheduled Date for Simulators; Monthly Calendar; Sponsor Evaluation Schedule; Team Evaluation Schedule; Qualification Time Line; Monthly Schedule Letter for Operators; Outstanding Evaluations; and Overdue Evaluations. None of the reports contain PII. The system audit reports occur at the server level and contain no PII.

[12] The URL associated with SIESS (https://afs600.avs.faa.gov/siess/SOQ) is used to find simulators that have been approved by FAA for training based on the simulator Statement of Qualifications. A limited number of sponsors use this URL. Currently the URL is inoperable.
[13] The SAS (CSAM ID 1996) PTA update was adjudicated by the DOT Chief Privacy Officer on 4/16/2018.
[14] The SPAS (CSAM ID 1422) PTA update is currently under development.
[15] The FAAMIS (CSAM ID 1981) PTA update is currently under development.

2 INFORMATION MANAGEMENT

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?

Members of the Public: SIESS contains the following personally identifiable information (PII): points of contact for sponsoring organization including:

- Name
- Business Address
- Sponsor ID (FAA designator)
- Office ID
- FSTD ID
- Email Address
- Fax Number
- Business Phone Number

Members of the DOT Federal Workforce: SIESS contains information for AVS Inspectors which includes:

- Name
- FAA Employment Code and a check box indicating whether the employee is active or not.
- Statements of Qualification (SOQ) uploaded to SIESS contain the signature of the FAA Manager of the NSP.

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

☒ **Yes**: The information on individuals in SIESS relates to information on simulator/FSTD sponsoring organizations and AVS inspectors.

☐ **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:

☒ **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:**

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 13, *Internet/Intranet Activity and Access Records*, May 7, 2002 67 FR 30757

☐ **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:

☐ **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:**

SIESS exchanges data with the following DOT/FAA systems:

- FAAMIS –FAAMIS maintains Flight Standards Service (AFS) information on air carriers, air agencies, and airmen and allows Aviation Safety Inspectors (ASIs) to research and report on aviation safety inspections. SIESS sends flat files of simulator data to a server that FAAMIS accesses to retrieve the information. FAAMIS uses SIESS simulator information as a definitive source of information regarding the status of simulator and FSTD evaluations for safety inspectors, supervisors, and safety analysts. This is a one-way data flow. No PII data is processed or exchanged during this interconnection and therefore no SORN coverage is required
- SPAS – SPAS provides users the ability to search for and view information regarding aviation safety trends. SIESS sends data regarding the status of simulator evaluations to a server that SPAS access. SPAS uses the SIESS information as a measure of safety performance used to identify potential problems. This is a one-way data transfer. No PII data is processed or exchanged during this interconnection and therefore no SORN coverage is required
- SAS - SAS supports the FAA by monitoring and managing aviation certificate holders as well as applicants for aviation certificates (CH/As). CH/As include airmen, air carriers, commuter airlines, repair stations and other relevant business entities. SIESS sends the following data elements to a server that SAS retrieves data from on a weekly basis: Simulator ID, as well as the type of aircraft that the training data supports and simulator location. SAS uses SIESS data to assist in

assessing CH's aircraft. No PII data is processed or exchanged during this interconnection and therefore no SORN coverage is required

- AIT Directory Services – Users access SIESS through their FAA Domain ID/Active Directory account used to log on to their workstation. The application is PIV-enabled, via Integrated Windows Authentication (IWA). PIV information such as PIV card serial number does not traverse the system boundary and is not stored in the system. An FAA Directory Services PTA was adjudicated September 28, 2018. SORN coverage is DOT/ALL 13, *Internet/Intranet Activity and Access Records*, May 7, 2002 67 FR 30757.

☐ **No**

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

☒ **Yes:**

Schedule Identifier: National Archives and Records Administration, General Records Schedule 3.1, Approved January 2017, General Technology Management Records.

Schedule Summary:

This schedule covers records created and maintained by Federal agencies related to the general management of technology. It includes records related to developing, operating, and maintaining computer software, systems, and infrastructure improvements; complying with information technology policies and plans; and maintaining data standards**.**

Item 020 - Information technology operations and maintenance records. Information Technology Operations and Maintenance records relate to the activities associated with the operations and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications.

Disposition: Temporary. Destroy 3 years 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. DAA-GRS-2013-0005-0004.

Schedule Identifier:

National Archives and Records Administration, General Records Schedule 3.2, Approved September 2016, Information Systems Security Records.

Schedule Summary:

This schedule covers records created and maintained by Federal agencies related to protecting the security of information technology systems and data, and responding to computer security incidents. This schedule does not apply to system data or content**.** In the immediate case, those records pertain to FAA user authentication information.

Item 030 - System access records - Systems not requiring special accountability for access. These records are created as part of the user identification and authorization

process to gain access to systems. Records are used to monitor inappropriate systems access by users. These are user identification records generated according to preset requirements, typically system generated.

Disposition: Temporary. Destroy when business use ceases. DAA-GRS-2013-0006-0003.

☐ **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**: 1984.

☐ **No:**

☐**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**:

☒ **Other**: Since the date of adjudication of the PTA, SIESS' data exchange with the Air Transportation Oversight System (ATOS) has discontinued as the ATOS system was decommissioned . In addition, SIESS has been scheduled to convert to a completely web-based application. This transition will require the Personal Computer (PC) aspect of the system to sunset. The transition is scheduled to be completed in Fiscal Year (FY) 2018, but no specific date has been set. The Scheduling aspect of the system is also no longer in use, and SIESS currently only serves as a repository for information on simulators and associated contact information. In addition, it has been determined that the only information pertaining to individuals is business information used in a business capacity, such as the contact information for personnel in companies involved with simulators.

☐ **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):

Anticipated Date of Updated ATO:

☒ **No:** The date of the Initial Authority to Operate (ATO) for SIESS was 9/18/14. The system is currently operating with an expired ATO.

☐ **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

The Simulator Inventory and Evaluation Scheduling System (SIESS) supports the Office of Aviation Safety (AVS) National Simulator Program (NSP) in qualifying all simulators used to train pilots who operate in United States airspace. In addition, SEISS had an upgraded and SIESS will be used to schedule evaluations of these devices and act as a repository of information on simulators (e.g. site location, sponsor, manufacturer).

Department of Transportation Privacy Officer identified that SIESS collects personally identifiable information (PII) on individuals and constitutes a privacy sensitive system during the January 22, 2014 adjudication of the PTA. SIESS contains PII such as points of contact for sponsoring organization including name, address, business address, sponsor identification (FAA designator), email address, office ID, fax number, FSTD ID number, and business phone number. SIESS also contains information about AVS Inspectors which includes the individual's name, FAA Employment Code and a check box indicating whether the employee is active or not. It was also determined that a Privacy Impact Assessment (PIA) was not required as, the information collection relates to internal government operations.

Since the adjudication of the PTA, SIESS was upgraded and included several new module. None of the new modules collects any additional PII. Users access is covered by SORN coverage is DOT/ALL 13, Internet/Intranet Activity and Access Records, May 7, 2002 67 FR 30757. It has also been determine that information in the system is not retrieved by a unique identifier associated with an individual as reflected in the previous adjduciated PTA. Therefore SIESS is not subject to the Privacy Act. SIESS records are covered by General Records Schedule 3.1 Approved January 2017, General Technology Management Records and General Records Schedule 3.2, Approved September 2016, Information Systems Security Records.

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
System Owner	Craig Merrill	2/13/2018
General Counsel	Michael McKinley	4/5/2018

Information System Security Manager (ISSM)	None	None
Privacy Officer	Bud Gordon	8/10/2018
Records Officer	Kelly Batherwich	6/4/2018

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: 10/19/2018

DOT Privacy Office REVIEWER: Brian Bullock

DESIGNATION

☐ **This is NOT a Privacy Sensitive System**

☒ **This IS a Privacy Sensitive 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:***

☐ ***PIA is required.***

☐ ***System covered by existing PIA: <<****Identify PIA****>>***
☐ ***New PIA is required.*** **<<**Rationale**>>**
☐ ***PIA update is required. <<****Rationale****>>***

SORN

☒ ***SORN not required at this time.***

☐ ***SORN is required.***

☐ ***System covered by existing SORN:***
☐ ***New SORN is required. <<****Rationale****>>***
☐ ***SORN update is required. <<****Rationale****>>***

DOT PRIVACY OFFICE COMMENTS

The DOT Chief Privacy Officer (DOT CPO) has determined that the Simulator Inventory & Evaluation Scheduling System (SIESS) is a privacy sensitive system. The system was established in 1984 and a review of the system security package does not reveal Significant System Management Changes since 2002 that negatively impacting privacy risk, therefore no PIA requied.[16] The FAA is responsible for managing all PII in the system in accordance with the FIPPs and must take reasonable actions to ensure its appropriate collection, use, and protection.

NOTE: Access control records including user name (first name and last name), password, password retention status, account roles and account status (enabled / disabled) 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.

NOTE: In the previously adjudicated PTA the DOT CPO did not object to the FAA declaration that records in the system were protected by DOT/FAA 847, Aviation Records on Individuals, November 9, 2010 75 FR 68849. Based on updated information provided in this PTA, coverage under 847 is not appropriate.

POA&Ms

- *SI-12, Information Handling and Retention*

  Issue: The records schedules provided in the PTA do not cover the substantive business records maintained in the system. The referenced records schedules address only the management of the system, not the records maintained in the system. Requirement: Review the records in the system and develop a comprehensive file plan for them, including as necessary any proposed records schedules addressing substantive records of the system. Submit file plan and any proposed records schedules not previously approved by NARA to the DOT Records Officer. Timeline: 90 days.

NOTE: In its 2014 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.

The adjudicated PTA should be uploaded into CSAM as evidence that the required privacy analysis for this system has been completed and CSAM entries modified as appropriate to reflect the disposition.

The PTA should be updated not later than the next security certification and accreditation (C&A) cycle and must be approved by the DOT CPO 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.

[16] FAA assertion that records are "internal operations" is incorrect.