Privacy Threshold Assessment (PTA)

Federal Aviation Administration (FAA)
Air Traffic Organization (ATO)
ATO, Operations Support/Spectrum Assignment & Engineering Team (AJW-1/AJW-1C2)
Office of Spectrum Management Local Area Network (ASR-LAN)

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 Threshold 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,

[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.

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 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: Office of Spectrum Management Local Area Network (ASR-LAN)

Cyber Security Assessment and Management (CSAM) ID: 1625

SYSTEM MANAGER CONTACT Information:

Name: Timothy Pawlowitz Spectrum Assignment & Engineering Team, AJW-1C2

Email: timothy.j.pawlowitz@faa.gov

Phone Number: (202) 267-9739

Is this a NEW system?

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

Is there a PREVIOUSLY ADJUDICATED PTA for this system?

☒ **Yes:**

Date: 8/29/2012

☐ **No:**

1 SUMMARY INFORMATION

1.1 System TYPE

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

Unique Investment Identifier (UII): 021-1295029282

Cyber Security Assessment and Management (CSAM) ID: 1625

☐ **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)

☐ **New Collection**

☒ **Approved Collection or Collection Renewal**

☒ **OMB Control Number: 2120-0001**

☒ **Control Number Expiration Date: 09/30/2019**


FAA_Form_7460-1_AJV-1-050117.pdf


OMB Control No2120-0001.doc

☐ **Other:**

1.2 System OVERVIEW:

The Air Traffic Organization (ATO) Office of Operations Support/Spectrum Assignment & Engineering Team (AJW-1/AJW-1C2)is submitting a Privacy Threshold Assessment (PTA) update for the Office of Spectrum Management Local Area Network (ASR-LAN) system. The last adjudicated PTA was dated August 29, 2012. It was determined that the ASR-LAN is not a privacy sensitive system.

The following changes have occurred since the last adjudicated PTA which affect privacy risk:

- New subsystem is added into ASR-LAN system allowing it to support IOS-based tablets (IPAD).
- The WebFCR subsystem is a recently deployed, web-base application comprising new functionality added as an externally based frontend web interface. The Web Frequency Coordination Request (WebFCR) is designed to be a Central point of entry for Frequency Co-ordination Requests (FCRs) from the Internet, based at FAA.GOV. The FCR request application, allows a user to “create an account and login to submit a given FCR. The application uses the account data to provide follow-up communications contact information to the processing Spectrum engineers and FMOs, after the technical FCR data is sent to AFM for further action, engineering and approval as appropriate.
- The WebFCR application account registration process for external users is the origin and single use-case of the Personally Identifiable Information (PII) in the ASRLAN. This PTA update reflects that PII is captured for Members of the Public, Other Government Agencies, the U.S. Military, as well as FAA staff.

High-Level Description of the System/Privacy Impacts:

- **FIPS 199 Confidentiality Impact:** Moderate
- **Subjects of Collection:** Members of the Public. Other Government Agencies, Military Personnel, FAA and Contract Employees
- **Sensitivity of the PII:** Personally Identifiable Information (PII)
- **Other**: Mission Critical, Spectrum Engineering Support Non-NAS System

Paragraph 3: Description of System; Location

The Spectrum Engineering Services Office secures, manages, and protects all civil aviation radio frequency spectrum resources. It helps ensure the safe transport of all individual flights between airports is based on radio frequencies being available and interference free so that all of the aviation systems function properly. The FAA's Spectrum Engineering Services Office provides these fundamental services by ensuring radio frequency assets are always clear and available.

The mission of the Spectrum Engineering Services is providing assignment, engineering and protecting the radio frequency spectrum required to support civil aviation communications, navigation, and surveillance (CNS) services which includes the National Airspace System (NAS). The Spectrum Organization also ensures that the spectrum engineering requirements for new civil aviation CNS systems and functions are satisfied. Accomplishing this mission requires extensive studies and technical preparation; coordination within FAA; and participation as the U.S. aviation representative or key U.S. delegation member in FAA, U.S. Government and industry, and international civil aviation and telecommunications forums.

The ASR-LAN is largely located at FAA Building, 600 Independence Avenue, Washington, District of Columbia. It has support sites at the Mike Monroney Aeronautical Center, Oklahoma City, Oklahoma and the William J. Hughes Technical Center in Atlantic City, New Jersey.

The ASR-LAN is specifically is made up of the Local Area Network of spectrum engineering, applications, subsystems, tools and utility programs that support the planning, workflow management, frequency interference analysis, modeling, coverage analysis, signal evaluation and service volume validation for proper spectrum assignment within the required civil aviation bands.

Currently, the ASR-LAN is comprised of servers (inclusive of standbys), hosting these primary Spectrum applications:

- **Automated Frequency Manager (AFM)**
  - Agenda Voting subsystem, integrated National Telecommunications and Information Administration NTIA GMF data in AFM enables approval/disapproval workflow for frequency assignment actions which are submitted by all government agencies and managed by (NTIA). This application also serves as a means for interference analysis and conflict resolution of pending or proposed frequency allocations.
    - NTIA GMF data only, some frequency records may contain information such as Name and Digital Signatures, would be in record workflow comments.
- **Expanded Service Volume Management System (ESVMS)** is a workflow management and reference database system primarily for aviation procedures.
- **Web Facility Transmitting Authorization Application(WebFTA)**
  - SMTS is a mobile application which is designed primarily to support Spectrum engineers to process an assignment when they are at the field using iOS based mobile devices such as iPhone and iPad platforms. This mobility capability for FAA Spectrum automation permits the FAA Spectrum engineers, managers and Frequency Management Officers (FMO) are able to access real-time production information, when they are operating away from their primary workstation.
- **Radiation Hazard Reporting Tool (RADHAZ)** is used by EOSH staff to structure and normalize radio frequency measurements at key FAA facilities.
- **Web Frequency Coordination Request (WebFCR)**
  - The WebFCR is the central point of entry for Frequency Coordination Requests (FCRs) from the Internet at https://webfcr.faa.gov.
    - Limited PII is used only to create and manage user accounts and is also used for authentication. Includes: First & Last Name, Business E-Mail address, encrypted Password, Agency, and Business Phone Number
- **Canadian Coordination System**
- **Back Office System** is a collection of applications and utilities that support the Spectrum mission to manage frequency allocations for the NAS.

Typical Transaction:

The WebFCR is the Central point of entry for Frequency Coordination Requests (FCRs) from the public thru the FAA Public Internet site at https://webfcr.faa.gov. The user creates and logins to submit a given FCR. The application uses the account data to provide follow-up communications contact information to the processing Spectrum engineers and Frequency Management Officers (FMO), after the technical FCR data is sent to AFM for further action, including engineering and NTIA approval as appropriate.

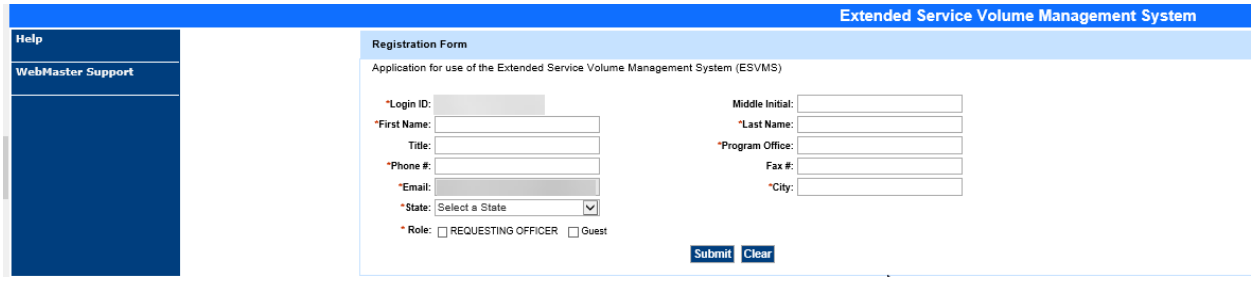
Users:

FAA Personnel, Other agencies, Military, Non-Federal persons.

- FAA and Contractor Administrators, including domain, system and domain administrators
- Other Privileged Users, including the Project Manager and Team Lead
- Military Personnel
- Personnel from Other Federal Agencies
- Members of the Public

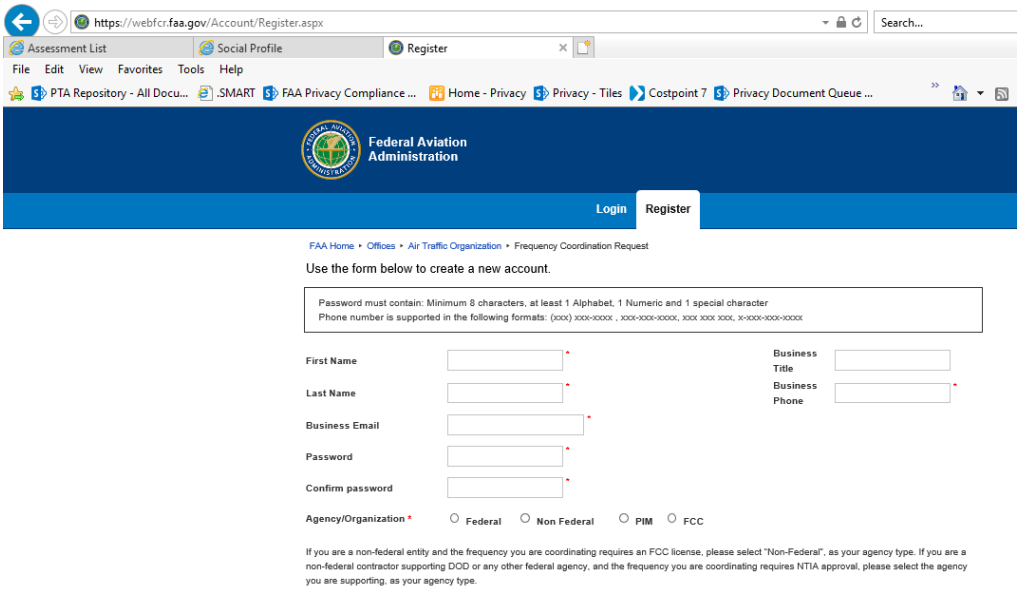
How Users Access System:

Internal FAA users authenticate to the system ~~Web based internet and web based intranet~~ via PIV card and the DOT/FAA My Access solution. Once at the application home page, internal FAA users are required to create an account.



External Users:

External users access the application through a public web site at https://webfcr.faa.gov.



Data:

The system and associated subsystems collect frequency request data and brief technical descriptions and parameters of the equipment which will be transmitting. The data is based on the equipment being deployed and aviation service proposed.

The system collects data provided by the user as part of their request for frequency coordination. Data accessed from other government agencies, such as elevation of the coordinates given from the *United States Geological Survey (USGS)* and *the existing frequencies being used via the Government Master File (GMF) from the National Telecommunications and Information Administration (NTIA)* .

(3) Describe How the Data is Protected:

The ASRLAN application is meticulously secured from all but senior database administrator success, and the application is protected with TLS, SSL and device hierarchical protocol security.
PII data isolated behind the firewall, with SSL 2048 bit encryption, with the user password data encrypted within the sub-system. The PII incident is only for account management and isolated processing purposes, no data is shared with any element of the application or process workflow.

Interconnections/Memorandum Of Understanding/Privacy Sharing Agreements:

Internal

- Intranet-Based Radio Coverage Analysis System (iRCAS)
- eNASR, subsystem of National Airspace System Resource System (NASR)

External:

- National Telecommunications and Information Administration (NTIA)
- United States Geological Survey (USGS)

Reports:

There are no reports from the system and no PII is reported in any form. Online dashboard gives the user the status of the request via a status code.

Forms:

FAA Form 7460-1 has been replaced by web application WebFCR.

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?

Members of the Public:

- First and Last Name
- Business E-Mail address
- Password
- Agency
- Business Title
- Business Phone number

Other Government Agencies and Military:

- First and Last Name
- Business E-Mail address
- Password
- Agency
- Business Title
- Business Phone number

Members of the FAA and Contract Workforce:

- Login ID, which is the user's government email address
- First, Middle Initial and Last Name
- Program Office
- Title
- Role
- Business Phone and Fax number
- Business E-Mail address
- City, State

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

☒ **Yes**:

- Limited PII data is collected for account creation and authentication purposes.

- The system captures audit logs which can identify the user.[3]

☐ **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*, 67 FR 30757 May 7, 2002

[3] Not all audit log functions are in place. This vulnerability is being tracked in the ATO Security Management and Assessment Reporting Tool (SMART) system.

SORN: DOT/ALL 16, *Mailing Management System*, 71 FR 35319 June 19, 20016

☐ **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 INTERNAL (DOT) or EXTERNAL (non-DOT) system or business activity?

☒ **Yes:**

System Name	External to FAA	Protocol?	Data Flow / Direction?	What Data is Exchanged ?	ISA/MOU Required?	Adjudicated PTA?
United States Geological Survey (USGS) Web Services	Yes	Web Service Read	Incoming,	Elevation data	No	N/A
NTIA	Yes	Internet	Both	GMF	Yes	N/A
Extended Service Volume Management System (ESVMS)	No	TCP	Bi-directional	None	No	N/A
Intranet-Based Radio Coverage Analysis System (iRCAS)	No	SSL	Outgoing	Links	No	N/A
eNASR, subsystem of National Airspace System Resource System	No	SSL	Incoming	Runway	No	N/A

☐ **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:**

Schedule Identifier:

Schedule Summary:

Disposition:

NOTE: Any unscheduled records, and records with schedules pending NARA's approval, must be kept indefinitely until NARA has approved the applicable schedule.

☐ **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**: 1997

☐ **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**:

- New subsystem is added into ASR-LAN system allowing it to support IOS-based tablets (IPAD).
- The WebFCR subsystem is a recently deployed, web-base application comprising new functionality added as an externally based frontend web interface. The Web Frequency Coordination Request (WebFCR) is designed to be a Central point of entry for Frequency Co-ordination Requests (FCRs) from the Internet, based at FAA.GOV. The FCR request application, allows a user to "create an account and login to submit a given FCR. The application uses the account data to provide follow-up communications contact information to the processing Spectrum engineers and FMOs, after the technical FCR data is sent to AFM for further action, engineering and approval as appropriate.
- The WebFCR application account registration process for external users is the origin and single use-case of the Personally Identifiable Information (PII) in the ASRLAN. This PTA update reflects that PII is captured for Members of the Public, Other Government Agencies, the U.S. Military, as well as FAA staff.

☐ **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): 3/17/2016

Anticipated Date of Updated ATO: 9/30/2019

☐ **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: Margarette

Email: Ebate

Phone Number: 202-267-7181

COMPONENT PRIVACY OFFICER Analysis

<< In addition to a review for overall completion, the Component PO analyzes the PTA, identifies any discrepancies in cited compliance activities, proposes resolutions, and addresses the need for additional privacy compliance documentation. Analysis identifies discrepancies in cited compliance activities and proposed resolutions. >>

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	Timothy J. Pawlowitz	02/26/2019
General Counsel	<<General Counsel Name>>	<<Review Date>>
Information System Security Manager Officer	Maryanne Chappell	03/06/2019
Privacy Officer	<<Privacy Officer Name>>	<<Review Date>>
Records Officer	Kristine Gorospe	<<Review Date>>

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