
U.S. Nuclear Regulatory Commission



Privacy Threshold Analysis PIV Peripherals System Subsystem of Automated Access Control and Computer Enhanced Security System (ACCESS)

**Office of Administration (ADM)
EA Number H0008**

**Version 1.0
09/25/2023**

Instruction Notes:

Please do not enter the PTA document into ADAMS. An ADAMS accession number will be assigned through the e-Concurrence system which will be handled by the Privacy Team

Template Version 2.0 (03/2023)

ACCESS PIV Peripherals	Version 1.0
Privacy Threshold Analysis	09/25/2023

Document Revision History

Date	Version	PTA Name/Description	Author
09/25/2023	1.0	PIV Peripherals PTA – Initial Release	ADM Oasis Systems, LLC
09/05/2023	DRAFT	PIV Peripherals PTA – Draft Release	ADM Oasis Systems, LLC

ACCESS PIV Peripherals	Version 1.0
Privacy Threshold Analysis	09/25/2023

Table of Contents

1	Description	1
2	Characterization of the Information	2
3	Records and Information Management-Retention and Disposal	4
4	Privacy Act Determination	7

ACCESS PIV Peripherals	Version 1.0
Privacy Threshold Analysis	09/25/2023

System/Project Name: PIV Peripherals.

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform)

None, PIV Peripherals stores no data.

Date Submitted for review/approval: 09/25/2023.

1 Description

1.1 Provide the description of the system/subsystem, technology (i.e., Microsoft Products), program, or other data collections (hereinafter referred to as “project”). Explain the reason the project is being created.

The PIV Peripherals system consists of hardware peripherals such as fingerprint scanners and cameras used to support the PIV Card Issuance Process (the process itself is not within the ACCESS FISMA boundary).

Please indicate if your project/system will involve the following:

<input type="checkbox"/> PowerApps	<input type="checkbox"/> Public Website
<input type="checkbox"/> Dashboard	<input type="checkbox"/> Internal Website
<input type="checkbox"/> SharePoint	<input checked="" type="checkbox"/> None
<input type="checkbox"/> Other	

1.2 Does this privacy threshold analysis (PTA) support a proposed new project, proposed modification to an existing project, or other situation? Mark appropriate response in table below.

Status Options	
<input type="checkbox"/>	New system/project
<input type="checkbox"/>	Modification to an existing system/project. <i>If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PTA and describe the modification.</i>
<input type="checkbox"/>	Annual Review <i>If making minor edits to an existing system/project, briefly describe the changes below.</i>
<input checked="" type="checkbox"/>	Other (explain) The ACCESS PIV Peripherals PTA is being split from the ACCESS consolidated PTA and updated to new template per NRC’s Privacy Officer’s request.

ACCESS PIV Peripherals	Version 1.0
Privacy Threshold Analysis	09/25/2023

1.3 Points of Contact:

	Project Manager	System Owner/Data Owner/Steward	ISSO	Executive Sponsor
Name	Denis Brady	Jennifer Golder	Tamar Katz	Jennifer Golder
Office /Division /Branch	Office of Administration (ADM) / Division of Facilities & Security (DFS) / Security Management and Operations Branch (SMOB)	Office of Administration (ADM)	Office of Administration (ADM) / Program Management, Announcements, & Editing (PMAE) / Budget & Information Technology Team (BITT)	Office of Administration (ADM)
Telephone	301-415-5768	301-287-0741	301-415-2500	301-287-0741

2 Characterization of the Information

Does this project collect, process, or retain information on: (Check all that apply)

Category of individual	
<input type="checkbox"/>	NRC Federal employees
<input type="checkbox"/>	Other Federal employees
<input type="checkbox"/>	Contractors working on behalf of NRC
<input type="checkbox"/>	Members of the Public (non-licensee workers, applicants before they are licenses etc.)
<input checked="" type="checkbox"/>	Project/system does not collect any personally identifiable information
<input type="checkbox"/>	Other

2.1 Is the project/system collecting information about an individual? If yes, provide a description of the information being collected.

N/A.

2.2 Please list the data fields/information being collected.

The ACCESS PIV Peripherals (Cameras and Fingerprint Scanners) do not store any information.

2.3 Does this project use or collect Social Security Numbers (SSNs)? (This includes truncated SSNs, such as the “last four.”)

N/A.

ACCESS PIV Peripherals	Version 1.0
Privacy Threshold Analysis	09/25/2023

2.4 Describe how the data is collected for the project. (i.e., NRC Form, survey, questionnaire, existing NRC files/ databases, response to a background check).

N/A.

2.5 If using a form to collect the information, provide the form number, title and/or a link.

N/A.

2.6 If the project/system shares information with any other NRC systems, identify the system, what information is being shared and the method of sharing.

N/A.

2.7 If the project/system connects, receives, or shares information with any external non-NRC partners or systems, identify what is being shared.

N/A.

Identify what agreements are in place with the external non-NRC partners or systems in the table below.

Agreement Type	
<input type="checkbox"/>	Contract Provide Contract Number:
<input type="checkbox"/>	License Provide License Information:
<input type="checkbox"/>	Memorandum of Understanding Provide ADAMS ML number for MOU:
<input type="checkbox"/>	Other
<input checked="" type="checkbox"/>	None

2.8 Describe how the data is accessed (NRC network/remotely) and the access control mechanisms that prevent misuse.

N/A.

2.9 Define the FISMA boundary this project/system is part of.

PIV Peripherals is a part of the ACCESS FISMA boundary.

2.10 Is there an Authority to Operate (ATO) associated with this project/system?

Authorization Status	
<input type="checkbox"/>	Unknown
<input type="checkbox"/>	No <i>If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Organization (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.</i>
<input type="checkbox"/>	In Progress provide the estimated date to receive an ATO. Estimated date:
<input checked="" type="checkbox"/>	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by

ACCESS PIV Peripherals	Version 1.0
Privacy Threshold Analysis	09/25/2023

<p>the Chief Information Security Officer (CISO) Confidentiality-Moderate Integrity- Moderate Availability- Moderate</p>
--

2.11 Provide the NRC system Enterprise Architecture (EA)/Inventory number. If unknown, contact [EA Service Desk](#) to get the EA/Inventory number.

The EA number is H0008.

3 Records and Information Management-Retention and Disposal

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are **Temporary** (eligible at some point for destruction/deletion because they no longer have business value) or **Permanent** (eligible at some point to be transferred to the National Archives because of historical or evidential significance). Records/data and information with historical value, identified as having a “permanent” disposition, are transferred to the National Archives of the United States at the end of their retention period. All other records identified as having a “temporary” disposition are destroyed at the end of their retention period in accordance with the NARA Records Schedule or the General Records Schedule.

These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR, agencies are required to establish procedures for addressing Records and Information Management (RIM) requirements. This includes strategies for establishing and managing recordkeeping requirements and disposition instructions before approving new electronic information systems or enhancements to existing systems.

The following questions are intended to determine whether the records/data and information in the system have approved records retention schedules and disposition instructions, whether the system incorporates RIM strategies including support for [NARA’s Universal Electronic Records Management \(ERM\) requirements](#), and if a mitigation strategy is needed to ensure compliance.

If the project/system:

- Does not have an approved records retention schedule and/or
- Does not have an *automated* RIM functionality,
- Involves a cloud solution,
- And/or if there are additional questions regarding Records and Information Management - Retention and Disposal, please contact the NRC Records staff at ITIMPolicy.Resource@nrc.gov for further guidance.

If the project/system has a record retention schedule or an automated RIM functionality, please complete the questions below.

ACCESS PIV Peripherals	Version 1.0
Privacy Threshold Analysis	09/25/2023

3.1 Does this project map to an applicable retention schedule in NRC’s Comprehensive Records Disposition Schedule (NUREG-0910), or NARA’s General Records Schedules?

<input type="checkbox"/>	NUREG-0910, “NRC Comprehensive Records Disposition Schedule
<input checked="" type="checkbox"/>	NARA's General Records Schedules
<input checked="" type="checkbox"/>	Unscheduled

3.2 If so, cite the schedule number, approved disposition, and describe how this is accomplished.

System Name (include sub-systems, platforms, or other locations where the same data resides)	PIV Peripherals System
Records Retention Schedule Number(s)	Not applicable, PIV Peripherals is just peripheral hardware with no data or records that are maintained. However, see suggested GRS 3.1 General Technology Management Records GRS 3.1 – 020 Information Technology Operations and Maintenance Records
Approved Disposition Instructions	*Note: Additional information/data/records kept in this system may need to be scheduled; therefore, NRC records personnel will need to work with staff to develop a records retention and disposition schedule for records created or maintained. Until the approval of such schedule, these records and information are Permanent. Their willful disposal or concealment (and related offenses) is punishable by fine or imprisonment, according to 18 U.S.C., Chapter 101, and Section 2071. Implementation of retention schedules is mandatory under 44 U.S. 3303a (d), and although this does not prevent further development of the project, retention functionality or a manual process must be incorporated to meet this requirement.

ACCESS PIV Peripherals	Version 1.0
Privacy Threshold Analysis	09/25/2023

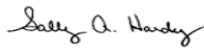
<p>Is there a current automated functionality or a manual process to support RIM requirements? This includes the ability to apply records retention and disposition policies in the system(s) to support records accessibility, reliability, integrity, and disposition.</p>	N/A
<p>Disposition of Temporary Records</p> <p>Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?</p>	N/A
<p>Disposition of Permanent Records</p> <p>Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions?</p> <p>If so, what formats will be used?</p> <p><u>NRC Transfer Guidance (Information and Records Management Guideline - IRMG)</u></p>	N/A

ACCESS PIV Peripherals	Version 1.0
Privacy Threshold Analysis	09/25/2023


4 Privacy Act Determination

Review Results		Action Items
<input checked="" type="checkbox"/>	This project/system does not contain PII.	No further action is necessary for Privacy.
<input type="checkbox"/>	This project/system does contain PII	A privacy impact assessment is required

Comments:

Reviewer's Name	Title
 Signed by Hardy, Sally on 10/11/23	Privacy Officer

I concur with this analysis.

 Signed by Harris, Kathryn
on 10/11/23

 Chief
 Cybersecurity Branch
 Governance and Enterprise Management
 Services Division
 Office of the Chief Information Officer