U.S. Nuclear Regulatory Commission

Privacy Threshold Analysis
Silo

Subsystem of Third Party System (TPS)
Office of the Chief Information Officer (OCIO)

Version 1.0
07/02/2025

Template Version 2.4 (04/2025)-ML091970114

Document Revision History

Date	Version	PTA Name/Description	Author
07/02/2025	1.0	Silo - Final Release	OCIO Oasis Systems, LLC
06/17/2025	DRAFT	Silo - Draft Release	OCIO Oasis Systems, LLC

Table of Contents

System/Project Name: Silo.

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform): Silo is externally hosted by Authentic8, data resides in a secure cloud environment in Council Bluffs, IA. For databases where persistent user data is stored, each is maintained as a high-availability primary and secondary cluster on a separate zone within Google's us-central1 region (Council Bluffs, IA).

Date Submitted for review/approval: July 10, 2025.

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.

Silo is a software-as-a-service (SaaS) cloud service offered by Authentic8. Silo is a remote browser that allows select NRC users to conduct anonymous online research from within an insulated container that is built directly into the browser. After NRC users exit the application, the container (search history, cookies, etc.) is destroyed.

Silo would also allow NRC staff to:

- perform research across geographies and web protocols, without concern over exposing identities; and
- save web content gathered from research within the Authentic8 Secure Storage encrypted repository.

Authentic8 is redefining how enterprises conduct business on the web with the Silo web isolation platform. Silo insulates and isolates all web data and code execution from user endpoints, providing powerful, proactive security while giving users full, interactive access to the web.

Silo is a subsystem of the Office of the Chief Information Officer (OCIO) Third Party System (TPS). TPS provides a framework for managing cybersecurity compliance for the external IT services used by NRC. TPS and its subsystems have no technical components on the NRC infrastructure.

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

☐ PowerApps	☐ Server/Database Design
☐ Dashboard	☐ Public Website
☐ SharePoint	☐ Internal Website
☒ Cloud Service Provider	☐ Artificial Intelligence (AI)
☐ External Sharing	☐ 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	
☒	New system/project
☐	Modification to an existing system/project. *If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PTA and describe the modification.*
☐	Annual Review *If making minor edits to an existing system/project, briefly describe the changes below.*
☐	Other (explain)

1.3 Points of Contact:

Role	Contact Information Name Office/Division/Branch Phone Number
Project Manager(s)	N/A
System Owner/Data Owner or Steward	Juan Jimenez Office of the Chief Information Officer (OCIO) / Cyber and Infrastructure Security Division (CISD) / Security Operations Branch (SOB) / Data and Identity Protection Team (DIPT) 301-287-0516
ISSM	Jonathan Butler Office of the Chief Information Officer (OCIO) / Cyber and Infrastructure Security Division (CISD) / Information Assurance and Oversight Branch (IAOB) 301-415-2560
Executive Sponsor	N/A
Other	

2 Characterization of the Information

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

	Category of individual
☐	NRC Federal employees
☐	Other Federal employees
☐	Contractors working on behalf of NRC
☐	Members of the Public (non-licensee workers, applicants before they are licenses etc.)
☒	Project/system does not collect any personally identifiable information
☐	**Other**

2.1 Please list the data fields/information being collected in the system. *For example (name, billing/financial information, conference registration information, medical information, education information, license numbers, business information, contact information, etc.***)**

Note: Response is required-not applicable is not an option.

Silo logs contain LAN IDs of the NRC staff and contractors who use the Silo Cloud web browser, along with the URLs they have visited using the Silo web browser.

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

No.

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

No.

2.4 Describe how the data is collected for the project. (i.e., NRC Forms, surveys, questionnaires, existing NRC files/ databases, via Artificial Intelligence, or electronic responses).

The data collected is the logs of who connects to the Silo service and the websites they visit. The Silo logs contain LAN IDs of the NRC staff and contractors who use the Silo Cloud web browser, along with the URLs they have visited using the Silo web browser.

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

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 Does the project/system connect, receive, or share information externally? If so, identify the system and what information is being shared and the method of sharing?

No.

Identify what agreements are in place with the external entities in the table below.

Agreement Type	
☐	Contract Provide Contract Number:
☐	License Provide License Information:
☐	Memorandum of Understanding Provide ADAMS ML number for MOU:
☒	Other: FedRamp ATO
☐	None

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

Silo is a remote browser that allows select NRC users to conduct anonymous online research from within an insulated container that is built directly into the browser. After NRC users exit the application, the container (search history, cookies, etc.) is destroyed.

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

Silo is a subsystem of TPS.

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

Authorization Status	
☐	Unknown
☐	No *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*.
☒	In Progress provide the estimated date to receive an ATO. Estimated date: TBD
☐	Yes **Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO)** Confidentiality

Authorization Status	
	Integrity Availability

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

N/A.

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.

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?

☐	NUREG-0910, "NRC Comprehensive Records Disposition Schedule
☒	NARA's General Records Schedules
☐	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)	Silo
Records Retention Schedule Number(s)	**GRS 4.2 item 030**, Information access and protection operational records. **GRS 4.2 item 031**, Information access and protection operational records. **GRS 4.2 item 032**, Information access and protection operational records.
Approved Disposition Instructions	**GRS 4.2 item 030** Temporary. Destroy 2 years after last form entry, reply, or submission; or when associated documents are declassified, decontrolled, or destroyed; or when an individual's authorization expires; whichever is appropriate. Longer retention is authorized if required for business use. **GRS 4.2 item 031** Temporary. Destroy when superseded or obsolete, but longer retention is authorized if required for business use. **GRS 4.2 item 032**, Temporary. Destroy 90 days after last entry on form, but longer retention is authorized if required for business use.
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	Silo will be assessed using the Records and Information (RIM) Certification process. The structured process will provide criteria aligned with the Suggested Rating to accurately reflect the system's ability to support records management requirements.

accessibility, reliability, integrity, and disposition.	
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	Automatically
Disposition of Permanent Records Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions? If so, what formats will be used? **NRC Transfer Guidance (Information and Records Management Guideline - IRMG)**	N/A

4 Privacy Act Determination

Review Results		Action Items
☒	This project/system **does not contain PII.**	No further action is necessary for Privacy.
☐	This project/system **does contain PII**	A privacy impact assessment is required
☐	Other	See comments section below for further details.

Comments:

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 07/29/25	Privacy Officer

I concur with this analysis.

Signed by Nalabandian, Garo on 07/31/25

Director
Chief Information Security Officer
Cyber Information Security Division
Office of the Chief Information Officer