U.S. Nuclear Regulatory Commission

Privacy Threshold Analysis
Exiger Federal Cloud (EFC)

Office of the Chief Information Officer (OCIO)

Version 1.0
09/15/2025

Template Version 2.4 (04/2025)-ML091970114

Document Revision History

Date	Version	PTA Name/Description	Author
09/15/2025	1.0	Exiger PTA - Final Release	OCIO Oasis Systems, LLC
09/03/2025	DRAFT	Exiger PTA - Draft Release	OCIO Oasis Systems, LLC

Table of Contents

System/Project Name: Exiger Federal Cloud (EFC).

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform): Data resides within the Exiger Federal cloud environment.

Date Submitted for review/approval: September 15, 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.

Exiger Federal Cloud is a FedRAMP authorized SaaS that provides supply chain risk management tools. It analyzes data related to software and hardware bill of materials to identify potential risks and vulnerabilities and risks associated with foreign ownership, control or influence. It includes risk factors such as reputational, criminal, regulatory, financial and operational. Exiger Federal Cloud provides a centralized platform for understanding complex relationships between suppliers to help identify potential risks. The products approved for use within the Exiger Federal Cloud are as follows:

- DDIQ - Conducts due diligence on companies and individuals within a supply chain.
- DDIQ Analytics - Assists with risk management and supply chain compliance.
- Supply Chain Explorer - Supply chain risk identification that includes over 50 risk categories.

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	Garo Nalabandian Office of the Chief Information Officer (OCIO) / Cyber and Infrastructure Security Division (CISD) 301-415-8421
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	Garo Nalabandian Office of the Chief Information Officer (OCIO) / Cyber and Infrastructure Security Division (CISD) 301-415-8421
Other	N/A

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.

Exiger collects the following data for individuals accessing the system: user's name, NRC email address, user's company's name and the reason for system access request. Data processed in Exiger includes company information related to NRC contracts or service providers including: Company name, address, DUNS number, and cage code.

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

Yes. The information collected about an individual consists of the user's name, NRC email address, user's company's name and the reason for system access request.

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).

For contractors utilizing Exiger, the information is collected on an Exiger vendor NDA form that is completed by the user.

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.

The Exiger vendor NDA form for contractors only.

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?

N/A.

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: Exiger Statement of Work (SOW)
☐	None

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

NRC users access the Exiger web-based portal via the Internet. The users are authenticated through the NRC's Identity, Credential, and Access Management (ICAM) Authentication Gateway, and they log into Exiger using a Single Sign-on from the NRC network.

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

Exiger is a component of the NRC's Third-Party System (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*.

Authorization Status	
☐	In Progress provide the estimated date to receive an ATO. Estimated date:
☒	Yes, Short -Term Authorization for Exiger through 4/30/2026 **Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO)** Confidentiality - Low Integrity - Low Availability - Low

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

The Exiger EA number is 20250002.

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)	Exiger Federal Cloud
Records Retention Schedule Number(s)	GRS 3.1, Item 011: System Development Records. GRS 3.1, Item 040: Information technology oversight and compliance records. Unscheduled
Approved Disposition Instructions	**GRS 3.1, Item 011:** Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use. **GRS 3.1, Item 040:** Temporary. Destroy 5 years after the project/activity/ transaction is completed or superseded, but longer retention is authorized if required for business use. **Unscheduled** 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.
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.	Exiger Federal Cloud 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.
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	Automatically Exiger Federal Cloud 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.
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
Signed by Hardy, Sally on 11/17/25	Privacy Officer

I concur with this analysis.

Signed by Nalabandian, Garo on 12/01/25

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