

## U.S. Nuclear Regulatory Commission

### Privacy Impact Assessment

*Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.*

#### Enterprise File Synchronization and Sharing (EFSS)

**Date:** December 10, 2021

#### **A. GENERAL SYSTEM INFORMATION**

- 1. Provide a detailed description of the system:** *(Use plain language, no technical terms.)*

The Enterprise File Synchronization and Sharing (EFSS) system is a cloud-based system that enables collaborative authoring and sharing of documents on a secure collaboration platform (Box) hosted by Box, Inc. EFSS is the U.S. Nuclear Regulatory Commission's (NRC)'s implementation of the Box Software as a Service (SaaS) solution.

EFSS is a secure method for collaboration and sharing of documents between the NRC internal users (NRC staff and contractors) and authorized external parties such as NRC licensees, other Federal agencies, NRC job applicants, etc. EFSS provides file synchronization and sharing that makes collaboration effective across devices, teams, and organizations. The system is not permitted to be used for long-term storage of agency documents and is set to retain documents for only 90 days unless an extended retention period has been approved.

EFSS is accessible through a web browser; it does not require any additional software or hardware to be installed by the user. In addition, EFSS users have the option to use Box Edit, an add-on feature that allows users to open and edit files stored in Box using the default applications installed on their computers. EFSS users can open and edit Microsoft Office files stored in EFSS using their desktop Microsoft Office applications.

The NRC internal users are authenticated to the Box Platform through the NRC Identity, Credential, and Access Management (ICAM) Authentication Gateway's single sign-on (SSO). Once authenticated, users with elevated privileges can create folders in EFSS, upload files, and invite external partners to view/edit files to facilitate collaboration. External recipients must accept the invitation sent via email by the system and create an account in the Box Platform within 90 days in order to access EFSS content. The Office of the Chief Information Officer (OCIO) EFSS system administrator (SYS ADMIN), NRC Program Office (Office) EFSS administrators (Office ADMINS), and internal collaborators will have the

ability to establish file and folder permissions such as read-only, no print, write, and access expiration based on their account privileges.

The OCIO System Administrator will create a root folder for each Office upon request from that Office. Each Office will have the ability to manage the file and folder permissions within their root folder. The Office ADMINS can give users co-owner rights for sub-folders under the root folder within EFSS that allow the user to establish external collaboration projects and upload documents to the subfolder(s) for access by external parties.

EFSS is a subsystem of the 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.

**2. What agency function does it support? (How will this support the U.S. Nuclear Regulatory Commission's (NRC's) mission, which strategic goal?)**

EFSS supports secure file sharing and collaboration for NRC users that need to collaborate with parties and organizations outside the NRC. EFSS provides a secure solution for sharing documents between NRC users and authorized external recipients.

**3. Describe any modules or subsystems, where relevant, and their functions.**

EFSS does not contain any modules or subsystems.

**a. Provide ADAMS ML numbers for all Privacy Impact Assessments or Privacy Threshold Analysis for each subsystem.**

N/A.

**4. What legal authority authorizes the purchase or development of this system? (What law, regulation, or Executive Order authorizes the collection and maintenance of the information necessary to meet an official program mission or goal? NRC internal policy is not a legal authority.)**

Part of the NRC's mission is official information dissemination, i.e., to share information from NRC staff members to authorized external users that rely on NRC-provided information. EFSS supports secure file sharing and collaboration for NRC users that need to collaborate with parties and organizations outside the NRC. Box provides a cloud platform that ensures the secure transmission of information shared with external parties.

**5. What is the purpose of the system and the data to be collected?**

All data stored in EFSS is solely for the purpose of sharing and collaborating within individuals and entities outside of the NRC in support of the NRC mission.

6. **Points of Contact:** (*Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary.*)

<b>Project Manager</b>	<b>Office/Division/Branch</b>	<b>Telephone</b>
Roy Choudhury	OCIO/ITSDOD/ADSB/CCAT	301-415-7226
<b>Business Project Manager</b>	<b>Office/Division/Branch</b>	<b>Telephone</b>
N/A	N/A	N/A
<b>Technical Project Manager</b>	<b>Office/Division/Branch</b>	<b>Telephone</b>
Roy Choudhury	OCIO/ITSDOD/ADSB/CCAT	301-415-7226
<b>Executive Sponsor</b>	<b>Office/Division/Branch</b>	<b>Telephone</b>
Thomas Ashley	OCIO/ITSDOD	301-415-0771
<b>ISSO</b>	<b>Office/Division/Branch</b>	<b>Telephone</b>
Natalya Bobryakova	OCIO/ITSDOD	301-287-0671
<b>System Owner/User</b>	<b>Office/Division/Branch</b>	<b>Telephone</b>
Thomas Ashley	OCIO/ITSDOD	301-415-0771

7. **Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?**

- a.  New System  
 Modify Existing System  
 Other

- b. **If modifying or making other updates to an existing system, has a PIA been prepared before?**

Yes.

- (1) **If yes, provide the date approved and the Agencywide Documents Access and Management System (ADAMS) accession number.**

ML20085F054; April 16, 2020.

- (2) **If yes, provide a summary of modifications or other changes to the existing system.**

Annual update to the newest template and changes made to the Points of Contact (POC) list. Update to system description and security controls to include the optional use of Box Edit Tool.

8. **Do you have an NRC system Enterprise Architecture (EA)/Inventory number?**

Yes.

- a. **If yes, please provide the EA/Inventory number.**

EFSS is a subsystem of the NRC's TPS. The TPS EA number is 20180002.

- b. **If no, please contact [EA Service Desk](#) to get the EA/Inventory number.**

## **B. INFORMATION COLLECTED AND MAINTAINED**

*These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.*

### **1. INFORMATION ABOUT INDIVIDUALS**

- a. **Does this system maintain information about individuals?**

EFSS documents can contain information about individuals if that information is needed for performing NRC business and mission critical functions. However, the information about an individual is not retrievable in EFSS by a personal identifier. All information in EFSS, including any information about individuals, is only disclosed to those with a need-to-know. Box encrypts all customer data and uses access control mechanisms to protect the information once a document is uploaded to the platform.

- (1) **If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public (provide description for general public (non-licensee workers, applicants before they are licenses etc.)).**

EFSS could contain information about Federal employees, Federal contractors, and licensees if that information is needed to perform NRC business and mission critical functions.

**(2) IF NO, SKIP TO QUESTION B.2.**

- b. What information is being maintained in the system about an individual (be specific – e.g., Social Security Number (SSN), Place of Birth, Name, Address)?**

The files placed in EFSS can contain any identifiable information about an individual if it is needed for business functions. This information may include an individual's name, address, phone number, date of birth, place of birth, social security number, or driver's license number; and any other information that is linkable to an individual, such as employment information. This information can be retained in the system for no longer than 90 days, unless a business justified exception for longer retention is approved by the NRC. EFSS is not permitted to be used for long-term data storage.

- c. Is information being collected from the subject individual? (To the greatest extent possible, collect information about an individual directly from the individual.)**

Yes. The files placed in EFSS may contain information collected from the subject individual or from other parties on behalf of an individual. However, in most cases, this information is collected outside of EFSS.

**(1) If yes, what information is being collected?**

Information about subject individuals may include an individual's name, address, phone number, date of birth, place of birth, social security number, driver's license number, or employment information.

- d. Will the information be collected from individuals who are not Federal employees?**

Yes. The files placed in EFSS can contain information collected from individuals who are not Federal employees. However, in most cases, this information is collected outside of EFSS.

**(1) If yes, does the information collection have the Office of Management and Budget's (OMB) approval?**

No Information Collection Request (ICR) is submitted. EFSS is used for file sharing. This is not information collection under the Paperwork Reduction Act (PRA).

**(a) If yes, indicate the OMB approval number:**

N/A.

**e. Is the information being collected from existing NRC files, databases, or systems?**

Yes. The information shared in EFSS may originate from other NRC systems or databases. However, EFSS is not directly interconnected with any other systems.

**(1) If yes, identify the files/databases/systems and the information being collected.**

The information shared in EFSS can originate from any existing NRC file, database, or information system.

**f. Is the information being collected from external sources (any source outside of the NRC)?**

The files placed in EFSS can originate from external sources, but EFSS has no direct interconnection with any external data sources.

**(1) If yes, identify the source and what type of information is being collected?**

The files placed in EFSS may contain any information that is needed for performing NRC business functions. The information from external data sources can be provided by other agencies, organizations, licensees, or members of the public.

**g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?**

Each Office / NRC Region is responsible for verifying the information they upload to/download from EFSS.

**h. How will the information be collected (e.g., form, data transfer)?**

The information is uploaded into EFSS by secure file transfer.

**2. INFORMATION NOT ABOUT INDIVIDUALS**

**a. Will information not about individuals be maintained in this system?**

Yes.

**(1) If yes, identify the type of information (be specific).**

EFSS is used for NRC's sharing information with the external stakeholders. The type of information maintained in EFSS is limited to what is permitted by each respective Office and must be compliant with existing agency guidance on sharing information externally. The information not about individuals could include

test data, reports, computer source code, and analytical results in binary formats.

**b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.**

The external sources of information could include other Federal agencies (e.g., the Department of Energy National Laboratories) and Federal and commercial contractors. Agency internal sources could include any NRC information system up to a Moderate impact level per Federal Information Processing Standards Publication (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems."

All information stored in EFSS is only intended for the temporary storage of general-purpose documents. Users cannot use EFSS as the primary storage resource for agency documents.

**C. USES OF SYSTEM AND INFORMATION**

*These questions will identify the use of the information and the accuracy of the data being used.*

**1. Describe all uses made of the data in this system.**

EFSS is used to securely share information with entities outside of the NRC. Each Office will be able to establish sub-folders for collaboration projects within the Office root folder. Each Office will also have an Office Administrator that will facilitate and administer collaboration projects and usage policies within the respective Office.

**2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?**

Yes, the use of the data in EFSS is both relevant and necessary for secure information sharing between NRC and external entities in support of NRC business and mission critical functions.

**3. Who will ensure the proper use of the data in this system?**

EFSS internal users within each NRC Office are responsible for reviewing the content stored in EFSS to ensure that they use the system only for authorized purposes and in compliance with the Agencywide Rules of Behavior for Authorized Computer Use and the EFSS Rules of Behavior for Internal Users. The external users would use the EFSS data under the same terms as if NRC staff had shipped the data to them on portable electronic media or emailed an encrypted file to them.

**4. Are the data elements described in detail and documented?**

Yes.

**a. If yes, what is the name of the document that contains this information and where is it located?**

The EFSS System Architecture Document (ML18137A476) describes the data elements in EFSS.

**5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?**

No.

*Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.*

*Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).*

**a. If yes, how will aggregated data be maintained, filed, and utilized?**

N/A.

**b. How will aggregated data be validated for relevance and accuracy?**

N/A.

**c. If data are consolidated, what controls protect it from unauthorized access, use, or modification?**

N/A.

**6. How will data be retrieved from the system? Will data be retrieved by an individual's name or personal identifier (name, unique number or symbol)? (Be specific.)**

Data can be retrieved from EFSS by viewing or downloading shared files. Data cannot be retrieved from shared files by an individual's name or a personal identifier. The EFSS SYS ADMIN can retrieve an event history of a user account by an individual's name.

**a. If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**

N/A.



**7. Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?**

No.

**a. If “Yes,” provide name of SORN and location in the Federal Register.**

N/A.

**8. If the information system is being modified, will the SORN(s) require amendment or revision?**

No.

**9. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?**

No.

**a. If yes, explain.**

N/A.

**(1) What controls will be used to prevent unauthorized monitoring?**

N/A.

**10. List the report(s) that will be produced from this system.**

EFSS allows the EFSS SYS ADMIN to generate detailed audit reports that provide a history of all events relevant to EFSS user accounts.

**a. What are the reports used for?**

The reports are used to view the full history of user accounts to support EFSS auditing and accountability.

**b. Who has access to these reports?**

Only the EFSS SYS ADMIN can access these reports for all user account.

**D. ACCESS TO DATA**

**1. Which NRC office(s) will have access to the data in the system?**

The EFSS SYS ADMIN creates the root folders for all NRC Offices and will have access to view files and folders from all Office folders. Each Office ADMIN will have access to all data within their Office root folder and will have the ability to set access permissions for sub-folders within each Office.

**(1) For what purpose?**

Each Office/Region could request an Office/Region root folder in EFSS for their external collaboration needs. Each Office/Region ADMIN will manage sub-folders for their external collaboration projects under the root folder to allow users to securely share files that are authorized for release to external third parties.

**(2) Will access be limited?**

Access for internal users will be limited to the permissions set by the EFSS SYS ADMIN and by the Office/Region EFSS ADMINS. External users can only view/edit files that they have been invited to view/edit by an internal user with co-owner rights.

**2. Will other NRC systems share data with or have access to the data in the system?**

Other NRC systems do not directly interconnect with EFSS and do not have access to the data in EFSS. The internal users upload/download the files to/from EFSS from/to their workstation local drives or network drives using secure file transfer over a HyperText Transfer Protocol Secure (HTTPS) connection.

**(1) If yes, identify the system(s).**

N/A.

**(2) How will the data be transmitted or disclosed?**

The data is transmitted to/from EFSS via a secure HTTPS connection.

**3. Will external agencies/organizations/public have access to the data in the system?**

Yes.

**(1) If yes, who?**

EFSS is a file sharing and collaboration tool used to share data with parties outside of the agency which can include other agencies, organizations, and licensees.

**(2) Will access be limited?**

All external parties must be invited by NRC users with co-owner rights to view files in the system. Co-owners ensure that external collaborators are given the least possible privileges. The Office/Region ADMINS set permissions for which sub-folders internal users will be able to access and their level of permissions. Permissions include co-owner, editor, viewer, previewer, and uploader.

**(3) What data will be accessible and for what purpose/use?**

Users can only access data that they have been given permission to access by a user with co-owner rights to a file or folder. Access to any data in the system will be based on the individual user needs for collaboration projects.

**(4) How will the data be transmitted or disclosed?**

Internal users access the NRC Tenant on Box (which is cloud based) to upload files. A user with co-owner privileges can invite an external user to view or edit the uploaded file. Once the external user receives the invitation via email, they must register an account on Box and accept the invitation within 90 days in order to view the shared file.

**E. RECORDS AND INFORMATION MANAGEMENT (RIM) - 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). 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 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management and NARA's Universal Electronic Records Management requirements, and if a strategy is needed to ensure compliance.*

- 1) **Can you map this system to an applicable retention schedule in [NRC's Comprehensive Records Disposition Schedule \(NUREG-0910\)](#), or NARA's [General Records Schedules \(GRS\)](#)?**

Yes.

- a. **If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).**

- **For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to an approved file format for transfer to the National Archives based on their approved disposition?**

At this time, the records and information in EFSS will fall under the following General Records Schedule (GRS) authorities with a **90-day retention period as set by the agency**. This is the authority unless other retentions are approved by the Agency Records Officer (ARO).

GRS 5.2 item 010 – Transitory

Disposition Instruction: Temporary. Destroy when no longer needed for business use, or according to agency predetermined time period or business rule.

- EFSS has a default retention of 90 days; all records are deleted from EFSS after that period. The system is not permitted to be used for long-term storage of official agency records. EFSS is primarily intended for temporary file sharing and users are not permitted to use the system for long-term storage of agency documentary material.
- All documents uploaded to EFSS by NRC staff must be retrieved from the Agencywide Document Access & Management System (ADAMS) or another NRC record repository system.
- Users can request exceptions for the default retention; however, the official record must be maintained in a record retention system.
- Any user with co-owner rights can delete a record stored in EFSS. Any files stored in EFSS are deleted after the default retention period unless an approved exception is made by the ARO and executed by the EFSS SYS ADMIN.
- If an exception for the default retention has been made, the file owner must delete the information upon completion of the collaboration project or once the document is no longer needed.

- Records will only pertain to the NRC business mission.
- All records are automatically deleted after the default retention period and any files uploaded with the same name will replace the existing files. Files and folders are only retained for the period of collaboration which can involve editing data on a daily, weekly, or monthly basis.

[GRS 3.2 item 030 – System Access Records](#) will cover Event Histories and Audit Reports; see also Item 031.

Disposition Instruction: Temporary. Destroy when business use ceases. Collaboration Invitations can be covered by this GRS as well; see Section D.3.4 of this PIA.

- b. If no, please contact the [RIM](#) staff at [ITIMPolicy.Resource@nrc.gov](mailto:ITIMPolicy.Resource@nrc.gov).

## F. TECHNICAL ACCESS AND SECURITY

1. **Describe the security controls used to limit access to the system (e.g., passwords).**

EFSS is integrated with NRC Enterprise Single Sign-On (ESSO) which requires users to be authenticated with their Personal Identity Verification (PIV) cards and passwords while on the NRC network. Internal users can also access the system outside the network with their NRC credentials and one-time password (OTP) credentials.

In addition to the multifactor authentication, Office ADMINS can set access permissions under the Office root folder based on their need-to-know.

External collaborators sign in with a username and passwords and must receive an invitation from an NRC EFSS user with co-owner rights in order to view any files or folders in the system. Collaboration invitations expire automatically after 90 days.

Box Edit/Tool Edit external collaborators sign in using a Time-based One-time password (TOTP) authenticator.

2. **What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?**

External collaborators can only be granted access to specific files in the EFSS system. Internal users are responsible for ensuring that the external collaborators have the least permissions necessary for viewing shared documents.

**3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?**

Yes.

**(1) If yes, where?**

System access procedures, controls, and responsibilities are documented in the EFSS System Architecture Document (ML18137A476), the EFSS Subsystem Security Plan 3.0 (ML19326C627) the EFSS Rules of Behavior (ML18226A309), and the EFSS User Manual (ML18225A022).

**4. Will the system be accessed or operated at more than one location (site)?**

Since the system is hosted by an Internet cloud service provider, EFSS users can access the system from any location.

**a. If yes, how will consistent use be maintained at all sites?**

Internal users are still required to adhere to the Rules of Behavior when accessing the system outside the NRC network. NRC personnel accessing the system from the internal network and a non-NRC managed network must use multifactor authentication with PIV credentials or an OTP.

**5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?**

The EFSS SYS ADMIN will have full access to the NRC Box Tenants and the ability to manage root folders for individual Offices. The EFSS SYS ADMIN provision rights to the Office ADMINS who manage access for users within each Office root folder.

**6. Will a record of their access to the system be captured?**

Yes.

**a. If yes, what will be collected?**

The EFSS audit history includes the following events:

- A collaborator was added to a file or folder.
- A file or folder was downloaded.
- A file or folder was copied.
- A file or folder was marked as deleted.

- A file or folder was renamed.
- A file or folder was recovered out of the trash.
- Admin login.
- Login Success including time/date.
- Login Failure including time/date.
- Created user.
- Changed user roles.
- Downloaded.
- Moved.
- Deleted.
- Undeleted.
- Source IP.

**7. Will contractors be involved with the design, development, or maintenance of the system?**

Box, Inc. employs contractors in the design, development, and maintenance of the host platform, which is an Internet cloud-based SaaS system. NRC contractors support the implementation and maintenance of the NRC Tenants and the EFSS implementation on the Box host platform.

*If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or Personally Identifiable Information (PII) contract clauses are inserted in their contracts.*

- *Federal Acquisition Regulation (FAR) clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*
- *PII clause, “Contractor Responsibility for Protecting Personally Identifiable Information” (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

*If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or Personally Identifiable Information (PII) contract clauses are inserted in their contracts.*

- *Federal Acquisition Regulation (FAR) clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*
- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

**8. What auditing measures and technical safeguards are in place to prevent misuse of data?**

Audit logs capture user and administrator activities within EFSS as well as the date and time of the events. Users are required to use EFSS in compliance with the EFSS Rules of Behavior. When files are placed by NRC users into EFSS, the external collaborators will only be given editor privileges to files when necessary.

**9. Is the data secured in accordance with the Federal Information Security Management Act (FISMA) requirements?**

Yes, Box has received an Agency Authority to Operate (ATO) from the Federal Risk and Authorization Management Program (FedRAMP). The FedRAMP authorization requires that systems are secured in accordance with the FISMA requirements.

**a. If yes, when was Certification and Accreditation last completed? And what FISMA system is this part of?**

EFSS has received a periodic authorization as a TPS subsystem through April 30, 2022 (ML21343A362). Box Edit received an authorization as an addition to the EFSS system boundary on July 21, 2021 (ML21203A257).

**b. If no, is the Certification and Accreditation in progress and what is the expected completion date? And what FISMA system is this planned to be a part of?**

N/A.

**c. If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Office's (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.**

N/A.



**PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL**  
*(For Use by OCIO/GEMSD/CSB Staff)*

**System Name: Enterprise File Synchronization and Sharing (EFSS)**

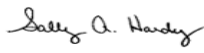
**Submitting Office: OCIO**

**A. PRIVACY ACT APPLICABILITY REVIEW**

- Privacy Act is not applicable.  
 Privacy Act is applicable.

**Comments:**

EFSS does not maintain personally identifiable information. All information in EFSS is encrypted during transition and at rest. Information is not retrievable by a personal identifier.


Reviewer's Name	Title
 Signed by Hardy, Sally on 12/16/21	Privacy Officer

**B. INFORMATION COLLECTION APPLICABILITY DETERMINATION**

- No OMB clearance is needed.  
 OMB clearance is needed.  
 Currently has OMB Clearance. Clearance No. \_\_\_\_\_

**Comments:**


EFSS itself does not need an OMB clearance since it is only a vehicle that is used to distribute and collect files. The EFSS users and EFSS Office administrators are responsible for ensuring that any use of EFSS is compliant with the requirements of the Paperwork Reduction Act.

Reviewer's Name	Title
 Signed by Cullison, David on 12/16/21	Agency Clearance Officer

**C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION**

- No record schedule required.
- Additional information is needed to complete assessment.
- Needs to be scheduled.
- Existing records retention and disposition schedule covers the system - no modifications needed.


**Comments:**

Reviewer's Name	Title
 Signed by Dove, Marna on 11/12/21	Sr. Program Analyst, Electronic Records Manager

**D. BRANCH CHIEF REVIEW AND CONCURRENCE**

- This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.
- This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

  
Signed by Nalabandian, Garo on 12/20/21

---

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

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/  
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

**TO:** Thomas Ashley, Office of the Chief Information Officer

**Name of System:** Enterprise File Synchronization and Sharing (EFSS)

**Date CSB received PIA for review:**

December 10, 2021

**Date CSB completed PIA review:**

December 16, 2021

**Noted Issues:**

EFSS supports secure file sharing and collaboration for NRC users that need to collaborate with parties and organizations outside the NRC. EFSS documents could possibly contain information about individuals if that information is needed for performing NRC business and mission critical functions. The information about an individual would not be retrievable in EFSS by a personal identifier. The EFSS information is encrypted during transition and at rest.

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

Signature/Date:



Signed by Nalabandian, Garo  
on 12/20/21

*Copies of this PIA will be provided to:*

*Thomas G. Ashley, Jr.  
Director  
IT Services Development and Operations Division  
Office of the Chief Information Officer*

*Jonathan R. Feibus  
Chief Information Security Officer (CISO)  
Office of the Chief Information Officer*