ADAMS ML18226A321

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: August 7, 2018

A. GENERAL SYSTEM INFORMATION

1. **Provide a detailed description of the system:**

The Enterprise File Synchronization and Sharing (EFSS) system is a cloud-based system that enables collaborative authoring and sharing of documents in a secure environment hosted by Box, Inc. EFSS is provided to the Nuclear Regulatory Commission (NRC) as a Software-as-a-Service (SaaS) solution. EFSS is a secure method for collaboration and sharing of documents between the NRC internal users and pre-approved external parties conducting regulatory business with the NRC such as licensees and other federal agencies. EFSS provides file synchronization and sharing that makes collaboration effective across devices, teams, and organizations. The system is not to be used for long-term storage of agency documents and is set to retain documents for only 30 days unless an extended retention period has been approved.

The Box Collaboration Platform is accessible through a web browser; it does not require any additional software or hardware to be installed by the user. 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 privilege can create folders in the NRC Box tenant, upload files, and invite external partners to view/edit files to facilitate collaboration. External recipients must create an account in the Box Platform and accept the invite within 90 days. The OCIO EFSS Administrators, Office EFSS Administrators, 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 EFSS Administrators will create a root folder for each office upon request. Each NRC program office will have the ability to manage the file and folder permissions within the root folder. Administrators can give users co-owner rights for subfolders within EFSS which allows the user to establish external collaboration projects and release documents to external parties.

EFSS 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.

2. **What agency function does it support?**

EFSS supports secure file sharing and collaboration for NRC users that need to collaborate with parties and organizations outside the NRC. EFSS provides a more secure alternative to clear-text email messages for sharing data with external recipients.

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

EFSS contains additional tenants used by the OCIO EFSS administrators for the development and testing of the system. These tenants do not contain any production data.

4. **What legal authority authorizes the purchase or development of this system?**

EFSS supports secure file sharing and collaboration for NRC users that need to collaborate with parties and organizations outside the NRC.

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 with entities outside of the NRC in support of the NRC mission.

6. **Points of Contact:**

Project Manager	**Office/Division/Branch**	**Telephone**
Eugenia Shyu	OCIO/ITSDOD	301-415-1396
Business Project Manager	**Office/Division/Branch**	**Telephone**
KG Golshan	OCIO/ITSDOD	301-415-5016
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Thomas Rich	OCIO/ITSDOD	301-287-0763
Administrator	**Office/Division/Branch**	**Telephone**
Scott Raimist	OCIO	301-415-7000

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

a. _X_ New System ___ Modify Existing System ____ Other (Explain)

b. **If modifying an existing system, has a PIA been prepared before?**

N/A

(1) **If yes, provide the date approved and ADAMS accession number**.

N/A

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

N/A

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?**

Most NRC offices at this time do not anticipate to use EFFSS for maintaining information about individuals. However, the EFSS documents could possibly contain information about individuals if that information is needed for performing NRC business and mission critical functions. However, the information about an individual would not be 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. The EFSS information is encrypted during transition and at rest.

(1) **If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).**

EFSS could contain information about Federal Employees, Federal contractors, and licensees if that information is needed for performing NRC business and mission critical functions and provided to only those authorized to use it for business needs.

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

b. **What information is being maintained in the system about an individual (be specific)?**

At this time, NRC is not planning to use EFSS for maintaining information about individuals. Potentially, the EFSS files could contain limited information about individuals if that information is needed for performing NRC business and mission critical functions.

c. **Is information being collected from the subject individual?**

No. EFSS cannot be used for collecting information from the subject individuals.

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

d. **Will the information be collected from 10 or more individuals who are not Federal employees?**

No. EFSS cannot be used for collecting information from 10 or more individuals who are not Federal employees.

(1) **If yes, does the information collection have OMB approval?**

N/A

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

N/A

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

EFSS cannot be used for collecting information about individuals from existing NRC files, databases, or systems.

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

N/A

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

EFSS cannot be used for collecting information about individuals from external sources.

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

N/A

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

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

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

The information is uploaded into EFSS by secure file transferring.

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 NRC Office and must be in compliance with existing agency guidance on sharing information externally. The information from the external sources 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. The 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 NRC office will be able to establish sub-folders for collaboration projects within the office root folder. Each NRC office will have an Office EFSS Administrator that will facilitate and administer collaboration projects and usage policies within the respective NRC office.

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

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?**

Internal EFSS users within each program 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 any applicable statute, rule, or regulation. The external users abide by the Information Sharing Agreements that NRC has with contractors and licensees who would access the data in EFFS. The external users would use the EFSS data under the same terms as if NRC staff had shipped the data to them on a DVD, 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

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

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

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

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

The data would not be retrievable from the system by an individual's name or a personal identifier. OCIO EFSS Administrators can retrieve an event history of a user account by an individual's name.

7. **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

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

EFSS allows the OCIO EFSS administrators 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 OCIO EFSS Administrators can access these reports for all user accounts.

D. ACCESS TO DATA

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

The OCIO EFSS administrators create the root folders for all NRC program offices and will have access to view files and folders from all office folders. Each Program Office Administrator will have access to all data within their office root folder and will have the ability to set access permissions for subfolders 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 EFSS administrator 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 OCIO EFSS administrators and by the office/region EFSS administrators. 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 share data with EFSS or 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 Hyper Text Transfer Protocol Secure (HTTPS) link. EFSS integrates with the NRC ICAM Authentication Gateway to authenticate internal users during logon.

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

N/A

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

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

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 any files in the system. Co-owners ensure that external collaborators are given the least possible privileges. The office/region EFSS administrators set permissions for which 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 upload files to the cloud system. 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 the Box Platform and accept the invitation within 90 days in order to view the shared file.

E. RECORDS 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 are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.

1. **Can you map this system to an applicable retention schedule in** NUREG-0910**, or the** General Records Schedules **at** http://www.archives.gov/records-mgmt/grs?

Yes.

a. **If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to a file for transfer 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 **30 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 020 – Transitory - Item 010

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 30 days and are deleted after 30 days. The system is not permitted to be used for retention or storage of official agency documents. 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 or official record storage.
- All documents uploaded to EFSS, must be stored in ADAMS or another NRC record retention 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 has the ability to delete a record stored in EFSS. Any files stored in EFSS are deleted after the 30 day retention period unless an approved exception is made by the Agency Records Officer (ARO) and OCIO EFSS administrators.
- If an exception 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 30 day retention period so any files uploaded with the same name will replace the existing files. Files and folders are only retained for the period which collaboration 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 the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

2. **If the records cannot be mapped to an approved records retention schedule, how long do you need the records? Please explain.**

3. **Would these records be of value to another organization or entity at some point in time? Please explain.**

4. **How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?**

5. **What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?**

6. **Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?**

7. **Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?**

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 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 Administrators have the ability to 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 a 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.

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 (ML18199A610), 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 a 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. Accessing the system either internally or externally requires users to use multifactor authentication with PIV credentials.

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

The OCIO EFSS administrators will have full access to the NRC Box tenants and have the ability to manage root folders for individual offices. The OCIO EFSS administrators provision rights to the Program Office Administrators 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?**

The cloud service provider employ contractors in the design, development, and maintenance of the cloud system. The NRC contractors support the implementation and maintenance of the NRC environment on the Box platform.

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. **Are the data secured in accordance with FISMA requirements?**

Yes, the Box Cloud system has received an ATO from the FedRAMP Joint Authorization Board (JAB). The JAB verified that the Box Collaboration Platform was secured in accordance with FISMA requirements.

a. **If yes, when was Certification and Accreditation last completed?**

EFSS has not yet received an ATO from the NRC.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL

(For Use by OCIO/GEMS/ISB Staff)

System Name: Enterprise File Synchronization and Sharing (EFSS)

Submitting Office: OCIO

A. PRIVACY ACT APPLICABILITY REVIEW

_X_ Privacy Act is not applicable.

____ Privacy Act is applicable.

Comments:

EFSS does not collect or 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	Date
Sally A. Hardy	Privacy Officer	9/20/2018

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

_X_ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No.________________

Comments:

EFSS as a system does not need an OMB clearance. Any collaborative effort between the NRC and the public using EFSS may be subject to the requirements in the Paperwork Reduction Act (PRA). Unlike issuing a Federal Notice, the use of EFSS to request comments or input on a document does not fall under the PRA exemption under 5 CFR 1320.3(h) for a general solicitation. OCIO policy is that the office using EFSS is responsible for ensuring they are complying with the PRA and other required regulations. It is highly recommended that the system owner (OCIO) provide guidance to users that reminds them of their responsibilities under the PRA, the Privacy Act, and Records Management requirements. The guidance should provide users with points of contact in these areas to assist them as needed

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	9/11/18

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

__X__ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	9/19/18

D. BRANCH CHIEF REVIEW AND CONCURRENCE

_X_ 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:

/RA Stephanie Blaney for/ Date 9/20/2018

Anna T. McGowan, Chief
Information Services Branch
Governance & Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/ PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Tom Rich, Information Technology Services Development and Operations Division, Office of the Chief Information Officer**

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

Date ISB received PIA for review: **August 14, 2018**	Date ISB completed PIA review: **September 20, 2018**

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.

If NRC has an operational need to use EFSS interactions or applications that are outside the scope of the requirements and analytical understanding outlined in this PIA, a separate or updated PIA must be written to address the specific privacy concerns that may be unique to that initiative.

Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA Stephanie Blaney for/** **9/20/2018**

Copies of this PIA will be provided to:

Tom Rich, Director
IT Services Development & Operation Division
Office of the Chief Information Officer

Jonathan Feibus
Chief Information Security Officer (CISO)
Governance & Enterprise Management Services Division
Office of the Chief Information Officer