United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev.2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usEPA.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Agency Records Management System (ARMS)	
Preparer: Greg Adams / Nannette Willis	**Office:** OMS/ORASE/ERMCD/CRTB
Date: 3/18/2025	**Phone:** 919-541-4297/ 443-889-7402
Reason for Submittal: New PIA____ Revised PIA__X__ Annual Review ____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☒	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

The Agency Records Management System (ARMS) is an agency-wide records management services infrastructure that provides electronic records management services for OneDrive, Desktop files, Office 365 e-mail, and paper records scanned through the Agency Digitization Centers. ARMS provides a set of core functional services that EPA users leverage for their daily business operations. ARMS allows end-users to submit files as records with assigned metadata. Submitted records are stored for long-term retention and shared among authorized EPA users.

ARMS is composed of three applications which include a Commercial off-the-shelf product (Nuxeo Studio) that provides much of the back-end functionality, an EPA developed user Interface (ARMS Uploader), and the Paper Asset Tracking Tool (PATT) that digitizes paper records at EPA Digitization Centers with copy machines. ARMS Uploader is a web-based user interface that allows end-users to select files within Outlook, OneDrive, from a

desktop, and other sources to submit as permanent records to Nuxeo. Additionally, PATT offers a second interface to allow large collections of paper files to be uploaded into Nuxeo. Files submitted via PATT and ARMS Uploader are ultimately stored records within MongoDB Software as a Service (SaaS) Database. However, PATT also has a dedicated AWS RDS MariaDB database that stores files submitted through PATT application and a different set of metadata that is stored within MongoDB. Nuxeo additionally provides a web-based user interface that allows EPA end-users the ability to search for shared records, change the metadata associated with submitted records that users have permissions to edit, and access a copy of shared records.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

CIO Memo 2135.0 Section 5 contains a list of specific legal authorities that permit and define the collection of information by ARMS. https://usEPA.sharepoint.com/:b:/r/sites/ECMS/Shared%20Documents/Intranet%20Migration/web/policy/cio21350.pdf?csf=1&web=1&e=10tE7B

- E-Government Act of 2002 (P.L. 107-347). Designed to enhance the management and promotion of electronic Government services and processes.
- Information Technology Management Reform Act (Clinger-Cohen Act). Public Law 104-106, 1996. – Provides the Agency's CIO responsibility for "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency" (Sec. 5125(b)(2)) and "promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency" (Sec. 5125(b)(3)).
- The Government Paperwork Elimination Act. Public Law 105-277, 1998. – Requires agencies to allow the public to interact with the federal government electronically, and to maintain records electronically when practicable. In addition, requires the establishment of strategic planning and performance measurement in the Federal Government.
- OMB Circular No. A-11, Part 7 on Planning, Budgeting, Acquisition and Management of Capital Assets – Encourages the use of enterprise-wide content management systems with capability to read records into the future to alleviate the need to maintain outdated software. OMB Circular No. A-130 – Management of Federal Information Resources

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes. 5/31/2028

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes, Amazon AWS, AWS IaaS provided by OITO

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

ARMS collects end-user submitted files through ARMS Uploader and PATT. The below table shows the mandatory set of metadata that must also be collected and associated with each file before it is submitted to the ARMS database.

Title	dc:title	Human-readable name of the asset. Should be in plain English and include sufficient detail to facilitate search and discovery.
Record Schedule	ARMS:record_schedule	A "records schedule" identifies records as either temporary or permanent.

Document Type	ARMS:document_type	Document type as defined by NARA: https://www.archives.gov/records-mgmt/policy/transfer-guidance-tables.html
Sensitivity	ARMS:sensitivity	Sensitivity of the Record. If No value the record will be stored as private records. Value of 1 means private 0 means shared.
Creation Date	ARMS:creation_date	Date the record was created.
EPA Contact	ARMS:EPA_contact	One or more EPA contacts.
Custodian	ARMS:custodian	The name of a contact responsible for the record.
Access Restriction	ARMS:access_restriction	Includes the following fields: Access Restriction Status, Specific Access Restrictions
Access Restriction Status	*ARMS:access_restriction_status*	*The indication of whether or not there are access restrictions on the archival materials.*
Specific Access Restrictions	*ARMS:specific_access_restrictions*	*Specific access restrictions to the archival materials, based on national security considerations, donor restrictions, court orders, and other statutory or regulatory provisions.*
Use Restriction	ARMS:use_restriction	Includes the following fields: Use Restriction Status, Specific Use Restrictions
Use Restriction Status	*ARMS:use_restriction_status*	*Indication of whether or not there are use restrictions on the archival materials.*
Specific Use Restrictions	*ARMS:specific_use_restrictions*	*Indicate whether or not there are use restrictions on the record.*
Program Office	ARMS:program_office	Tag derived from the Office Code. See ARMS Final Mapping spreadsheet.
AA'ship	ARMS:aa_ship	Office Code derived from the program office that specifies which workspace the file is saved under.
Record ID (UUID)		The unique record ID assigned by EPA's agency records management system. The UUID is the auto-assigned number generated by Nuxeo.
File Name		The complete name of the computer file including its extension (if present).
Litigation Hold	ARMS:lit_hold_flag	Determines whether a record is under litigation hold. 0 = False and 1 = True.
FOIA	ARMS:foia_flag	Determines whether a record is under a FOIA request. 0 = False and 1 = True.
Congressional	ARMS:congressional_flag	Determines whether a record is under a congressional request. 0 = False and 1 = True.
Inspector General	ARMS:ig_flag	Determines whether a record is under an Inspector General request. 0 = False and 1 = True.
Application ID	ARMS:application_id	Unique ID Provided by ARMS when application is registered for System to System Transfer.

Transfer Request Number		The number assigned by the National Archives and Records Administration's (NARA) Electronic Records Archives (ERA) when a request to transfer permanent records is submitted.

Please reference the following Nuxeo Data Model Spreadsheet for additional details and optional metadata fields that may also be collected.

2.2 What are the sources of the information and how is the information collected for the system?

The ARMS Nuxeo backend application receives records submitted through either the ARMS Uploader UI or PATT application. ARMS Uploader is a web interface that users can access to select emails, OneDrive files, or files located on their desktop. Once an end-user selects files to upload to ARMS Nuxeo, they must complete mandatory metadata fields within ARMS Uploader to ensure each uploaded file has the mandatory metadata assigned. Alternatively, at a designated EPA Digitization Center there are paper scanning devices that convert paper records into digitized records. Employees at the Digitization Centers receive boxes of paper records that have a Box List with mandatory metadata that needs to be gathered. The digitized records and Box List information is uploaded into PATT, sent to ARMS Nuxeo for processing, and stored within the ARMS MongoDB SaaS database.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No

2.4 Discuss how accuracy of the data is ensured.

ARMS Nuxeo application provides MD5 hashing for submitted records. Please see the following Nuxeo documentation for details on file storage MD5 hashing. Once records are submitted by end-users, the integrity of the submitted data is ensured using the hashing mechanism implemented within Nuxeo.

Individuals are responsible for accuracy of the information they submit to ARMS. All agency users can submit files they determine meet the requirements of an agency record. Annual training and intranet resources are provided to end-users to communicate their record management responsibilities and how to use the ARMS system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

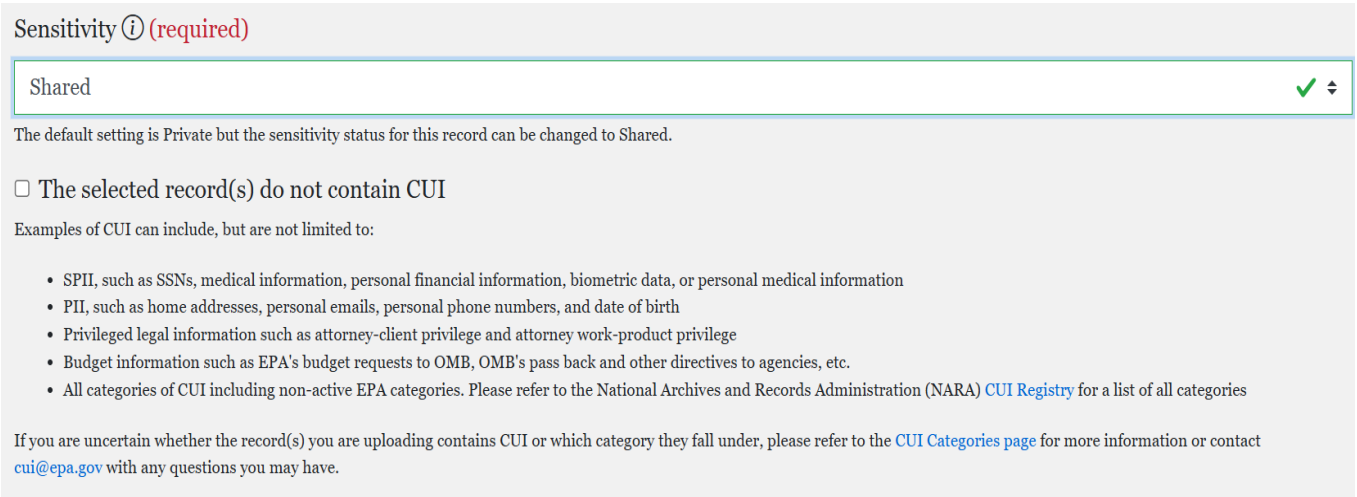
Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

The metadata captured for each file, as described in section 2.1 does not raise any privacy concerns. However, the actual files that are chosen and submitted by end-users to be stored as records, may contain CUI, including PII. There are legitimate use cases where end-users may submit sensitive files containing CUI, such as PII and CBI information. However, there are mitigating controls in place to prevent sensitive files from being shared among the submitting user's AA'ship.

Mitigation:

In addition to deploying NIST 800-53 controls, ARMS Uploader has several controls in place to prevent unintentional sharing of sensitive submitted records. To prevent end-users from unintentionally submitting and sharing sensitive files containing CUI, ARMS Uploader categorizes files selected for upload as "Private" by default. The "Private" designation only allows the submitter to view the record sent to ARMS, unless additional individual EPA contacts that should have access are listed. If the submitter of a record selects the "Shared" designation, it would then be accessible to that user's AA'ship once submitted. Users are presented with a mandatory prompt in ARMS Uploader certifying that they have reviewed the files to ensure there is no CUI contained within the files before being allowed to submit to ARMS.



With regards to PATT, there is a Box List that must be completed to designate whether any

included documents are sensitive and contain CUI. Before files are uploaded into PATT there are multiple fields that must be completed which specify whether CUI is included, whether the files require access restrictions or can be shared among the EPA Contact's AA'ship, and what specific individuals require access if access restrictions are identified. For a complete listing of the Box List metadata gathered for PATT processed files, please reference the PATT Box List Reference Guide.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes, access control levels are in place within ARMS to prevent unauthorized access to records. ARMS requires user accounts to be established in the system prior to a user being able to access the system for saving emails, searching emails or using any of the ARMS application management tools. All current EPA employees and contractors with email accounts have been set up with regular user accounts in the system. ARMS does not use guest/anonymous or temporary accounts. Membership in the regular user account allows a user to access the records classification screen to save an email record to their organization's records-keeping file plan. Any regular user can also save an email record to the Superfund record schedule. They can also access the ARMS arch screen to search for and view email records saved within their organization's records-keeping file plans. They can view records that they have saved as "sensitive" or private records.

See the following for a list of all ARMS custom group and roles

The records repository control encompasses the below set of roles for system users to ingest, manage, and dispose of agency records. The implementation of functions is carried out in the system using Nuxeo artifacts such as (groups, ACL's and security polices)

Records Contributor

Any active user (EPA staff/ EPA contractor) in ARMS system is called records contributor (custodian). Each records custodian should be assigned to a default user group which is defined by the AA' ship the user work for.

The users inherit following rights to the records

- Read: Shared records saved by users within AA 'ship group
- Read/Write: Shared and Private records where they are the custodian

Records Managers

Any active user (EPA Staff) is designated as a records liaison officer to manage agency records within their assigned AA ship group.

The users inherit following rights to the records

- Read: Shared and Private records saved by users within AA 'ship group
- Write: Shared and Private records saved by users within AA 'ship group
- Manage: Shared and Private records saved by users within AA 'ship group

System Administrator

Any active user (EPA staff/ EPA contractor) is designated as a power user to perform agency system administration, audit management, and help desk support for ARMS System.

The users inherit following rights to the records

Everything: All rights to manage Shared and Private records saved by users within the repository

Service Accounts

Accounts are created and are designated as a power user to ingest records into the system using API.

The users inherit following rights to the records

- Read/Write: Shared and Private records saved by users within the repository

Groups can be composed of users and sub-groups. Sub-group members automatically become members of the parent group. Thus, they are granted all the permissions system given to the group.

Admin group (ARMS-admin)

Any users designated as administrators added to the group as member

Example: PMO, Attorneys, Helpdesk Team etc.

Employee group (ARMS-EPA-employee)

Active EPA staff (Federal Employee) added to the group as member

Contractors group (ARMS-EPA-contractor)

Active EPA contractor, interns, or temporary staff (Non-Federal Employee) added

to the group as member

Service account group (ARMS-service-account)

Active service account designated for integration (svc accounts) added to the group as member

Example: Integration account for API (svc_patt, svc_ezdesktop etc.)

AA' ship-based group (21 groups – The group Name is (Office Code)**)**

Any active user (EPA staff/ EPA contractor) added to group as a member based on their organizational affiliation at EPA.

Example: For OMS the group name is "H0000000". All employee/contractor working for OMS and its sub organizations are member of this group

RLO AA' ship-based group (21 groups – The group Name is (" RLO-" Office Code)**)**

Any active user designated as RLO added to group as a member based on their organizational affiliation at EPA.

Example: For OMS the RLO group name is "RLO-H0000000". All OMS RLO's are member of this group

RLO general group (ARMS-rlo)

All AA' ship-based RLO group added to group as a member. This group is used for managing security

Records repository group (ARMS)

The ARMS-EPA-employee and ARMS-EPA-contractor group added to group as a member. This group is used for managing security

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

The access controls identified in 3.1 are documented in detail in EPA's Access Control Policy [located here] and ARMS Roles and Responsibilities 2024.docx

3.3 Are there other components with assigned roles and responsibilities within the system?

No, ARMS requires user accounts to be established in the system prior to a user being able to access the system for saving records, searching records or using any of the ARMS application management tools.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

All current EPA employees and contractors with email accounts have been set up with regular user accounts in the system. FAR 4.703 specifies that all federal contractors must retain certain project records for audit and inspection purposes. Section c provides express provision which allow contractor so "[duplicate or store] original records in electronic format."

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Records are retained until scheduled disposition of records from the system based on pre-defined records retention schedules.

Schedule: 0742

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

Records could be retained longer than authorized or removed prior to the pre-defined records retention schedule.

Mitigation:

Removal events are audited on a weekly basis by reports generated from the ARMS system. All deletions from the system are audited. The addition of records to the system is audited through weekly transaction reports and daily records transmission reports. The reports are maintained by the NCC ARMS system administrator and the EPA ARMS Records Management Technology Team.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

External access and sharing of records stored within ARMS is not allowed.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

Any future planned integration projects with other systems will require a signed Interconnection Security Agreement (ISA). The ISAs identify stakeholders, the responsibilities of the identified stakeholders, operations and maintenance roles, and additional memorandum of understanding requirements between both the Office of Mission Support (OMS) group managing ARMS and the group managing the interconnect system(s). Both the OMS Senior Information Officer (SIO) and the integrated system office SIO must sign the ISA before implementing in production.

4.4 Does the agreement place limitations on re-dissemination?

No, there are situations where some third-party systems process and disseminate information within the agency without the use of ARMS. The purpose of ARMS is to provide the agency with a centralized record management system for the agency. While some groups choose leverage ARMS as the only means to share information within the agency, others may have a reason to use another system to also share files and records within the agency.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

The Agency Records Management System is not accessible to users outside the agency. You

must be either logged into the VPN or connected to the local intranet to use the system. You must also be logged in via PIV credentials as an EPA employee or contractor.

Privacy Risk:

N/A

Mitigation:

N/ A

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy- based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

All transactions are tracked within ARMS through auditable events. The system does not alter the original content or time ordering of audit records. The system handles audit reduction and report generation capability by auditing functions within the database. The database creates customized reports based on the audit events in the system. These audit logs are reviewed to ensure that information is used in accordance with stated practices outlined in this PIA. The system is periodically assessed for risk and continuously monitored in line with NIST RMF.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

Only EPA employees and approved contractors may request access to this system, which means they have completed and passed Information Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Failure to log events or audit logs could be inadvertently lost.

Mitigation:

Database audit logs are kept for 90 days, some of that time on the instance and some of the time archived on a separate instance. Anything older than 90 days is deleted daily. In general, they are on the DB server for about 24 hours then moved to the backup appliance. Audit records generated

today would stay on the database for the rest of the day, then be moved to the separate database and kept for 90 days. The last backup of the separate database would be kept for another 90 days. That adds up to approximately 180 days' retention, 170 days to allow for the usual "expected" unexpected.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

In support of the authorities mentioned in section 1.1, ARMS performs the role of repository for EPA records and make them retrievable by EPA employees.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes__ No _X_. If yes, what identifier(s) will be used.

(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

[The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.]

We conduct periodic privacy impact assessments and continuously monitor the system.

6.4 <u>Privacy Impact Analysis</u>: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

<u>Privacy Risk</u>:

N/A

Mitigation:

N/A

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@EPA.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

N/A

Mitigation:

N/A

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their

information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

N/A

Mitigation:

N/A

I attest as the Agency Privacy Officer that the Agency Records Management System (ARMS) Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

Lee Kelly
Agency Privacy Officer
Division Director, ESPPD
OMS/OISP

ROBERT KELLY
Digitally signed by ROBERT KELLY
Date: 2025.11.04 07:51:53 -05'00'