United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – 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 Roster.docx

System Name: Email and Collaboration Solutions (ECS) HCL Notes		**System Owner:**	
Preparer: Lawrence Lee		**Office:** Office of Finance and Administration	
Date: January 28, 2026		**Phone:** (202) 566-1042	
Reason for Submittal:			
New: **X**	Revised:☐	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: **X**	
Operation & Maintenance: ☐	Rescindment/Decommission: ☐		

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:

National Notes and Mail (NNM) / HCL Notes, an Email and Collaborations Solutions (ECS) subsystem application, is an email application used by the EPA federal and contractor workforce since before 1990. With the Agency's switch to MS Exchange and Outlook starting in 2013, the HCL Notes mail platform has been replaced as the official email application for the EPA and only archived email remains

available for records and FOIA requests. The HCL Notes platform continues to support communication and collaboration between our EPA partners both inside and outside the Agency with the customized case management applications used by the Environmental Appeals Board (EAB), Office of Administrative Law Judges (OALJ), and Regional Hearing Clerks (RHC).

The organization responsible for the operation, management, and maintenance of the EPA NNM / HCL Notes platform is OFS/OITO/ECSD, located in Washington, DC.

The EAB, OALJ, and RHC custom applications are essential applications that allows for the EPA to manage and track the many EAB/OALJ/RHC decisions, orders, and filings that comes before the EPA.

Section 1. 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?

- 5 U.S.C. 301 "Departmental Regulations". The head of an Executive department or military department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property.

- 44 U.S.C. 3541 et seq., Federal Information Security Modernization Act of 2014. Codifies the Department of Homeland Security's role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies.

- 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)).

- 44 U.S.C. § 3506, which establishes federal agencies' responsibilities for managing information resources and 40 U.S.C. § 11315, which establishes the responsibilities of the agency's Chief Information Officer to manage agency information resources.

- OMB Circular No. A-130 – Management of Federal Information Resources. The Circular establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy. The Circular promotes innovation, enables appropriate information sharing, and fosters the wide-scale and rapid adoption of new technologies while strengthening protections for security and privacy.

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, a System Security Plan has been completed for HCL Notes, an sub-system application under ECS. The ECS system has an ATO that expires on October 31, 2026.

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, archived email dbs and archived applications data is supported and maintained in the MS Azure Cloud via a Windows Server hosting service. The MS Azure CSP is a FedRAMP approved IaaS.

Section 2. 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).

The identified information within the HCL Notes system is:

- Account Directory (AD) information
- Employee and Contractor names
- Work Address
- Work Telephone Number
- Work Email Address
- Workforce ID (WFID)

Within the customized EAB/OALJ/RHC legal case applications, the information collected is:

- Stored Internal Staff Contact Information
- Case Contact Information

Note: Copies of financial information for case plaintiffs and defendants which are also stored within the secured, access controlled customized legal case applications are not shared with the public.

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

HCL Notes sources of information come from Active Directory, requests through ServiceNow ticket system, as well as from e-Business to create the application accounts. The information copied from the e-Business account is:

- Name
- Phone Number
- Program Office or Region
- Email Address
- Workforce ID Number

2.3 The program applications may contain data with names, addresses, and phone numbers. Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, the system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Accuracy of the data must be ensured by each NNM account holder.

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:

There is a risk that the information collected from data sources such as Active Directory, etc. is outdated.

Mitigation:

Verifying accuracy of the data must be ensured by each NNM account holder.

Section 3. 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, all user access to HCL Notes requires ISO approval prior to account creation. Access is then granted via access control list and only for the level of access needed to prevent unnecessary elevated privileges to resource.

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

The procedures for how access is controlled for HCL Notes are documented under Access Control (AC) -2 in the ECS System Security Plan.

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

No, there are no other components with the assigned roles and responsibilities within HCL Notes.

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?

Both government and contractor employees have access to the data/information in HCL Notes. The appropriate FAR clauses, CFR 24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act, have been incorporated into the contract and provide a foundation for the contractor's privacy data protection policies.

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.

NNM retains emails for a period of at least 10 years for regular users and permanently for government officials and legal cases in accordance with EPA Records Schedule 0759 and 0760.

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:

There is a risk that HCL Notes is not meeting the Federal guidelines and requirements for records retention by a government information system.

Mitigation:

To mitigate this risk, HCL Notes have yearly reviews to make sure that it's meeting all applicable Federal guidelines, mandates and requirements related to the length of time data is retained in accordance with our EPA Record Schedules.

Section 4. 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.

Yes, information is shared outside the EPA as part of normal operations. There is legal case data that is shared by the Environmental Appeals Board, Office of Administrative Law Judges, and Regional Hearing Clerks. The data is made available to the public through the organization's website as deemed necessary by their respective organizations. This follows the intended use of the application.

Note: No financial data will ever be shared with the public.

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

FOIA or records requests (of archived email or archived application data) and production application usage based on the functionality developed and used for EAB, OALJ, and RHC processes. The three groups have their own processes in determining what should be or should not be shared with the public from their customized production applications.

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?

A formal FOIA request is needed. The approval of the request is done by the EAB, OALJ, and RHC management. There are no MOUs agreements.

4.4 Does the agreement place limitations on re-dissemination?

There are no MOU agreements in place.

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?

Privacy Risk:

Organizations may improperly share information (ex: copies of checks) to the public or with unauthorized users.

Mitigation:

The organization follows proper vetting procedures before disclosing information to the public sites and utilize access controls.

Section 5. 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?

EPA ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behaviour, and auditing and accountability. EPA security specifications require auditing capabilities that log the activity of each user to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All EPA systems employ auditing measures and technical safeguards to prevent the misuse of data.

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

The US EPA implements a Rules of Behavior (ROB) for which all users must consent prior to being granted systems credentials for access. The system inherits the EPA implementation of User Information Security and Privacy Awareness Training (ISAPT) which is provided annually. In addition, all EPA personnel receive annual refresher cybersecurity training to educate them regarding the use and management of sensitive data.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

There's a risk associated with auditing and accountability in relation to NNM that unauthorized access to audit records maintained could occur.

Mitigation:

Encryption mechanisms prevent information loss or theft audit data is stored in the underlying database files. All data is encrypted in transport and at rest.

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

NNM uses the data to support communication and collaboration between its partners, other agencies, and the public, however, no sensitive PII is shared with these other agencies.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: X No: ☐ 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.

The personal identifier used to retrieve information by the application is first name, last name, and email address.

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.

NNM application owner, application engineers and security team evaluate at least annually the types of data collected and stored within the system, at least monthly which users have access to the system and conducts a weekly review of the audit logs to identify any potential security breaches. During these processes, the probable or potential effect or impact to the privacy of individuals are assessed.

6.4 Privacy Impact Analysis: 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.

Privacy Risk:

There is a low risk of misuse of the system information, for example if an administrator directly or indirectly shares system information data by providing a name or phone number of an individual, that could allow an unauthorized individuals to receive data that is not meant to be shared.

Mitigation:

HCL Notes restricts all information based on a business need to know using role-based access controls, implemented multifactor authentication, and conducting weekly security audit log reviews. Access to customer data is also strictly logged and third party annual security assessments and audits (as well as sample audits) to attest that all access controls are meeting EPA's requirement and are appropriate.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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?

Click or tap here to enter text.

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:

Click or tap here to enter text.

Mitigation:

Click or tap here to enter text.

Section 8. 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 Freedom of Information Act (FOIA).

Privacy Risk:

Click or tap here to enter text.

Mitigation:

Click or tap here to enter text.

I attest as the Agency Privacy Officer that **Email and Collaboration Solutions (ECS) HCL Notes's** 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,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.03.17 11:27:48 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA