United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 12/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: National Hosting Services (NHS)	
Preparer: Jeffrey Lane	**Office: OMS/ITSSS**
Date: 12/20/2019	**Phone: 202.566.1807**
Reason for Submittal: New PIA____ Revised PIA__X__ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s): Operations & Maintenance	
Definition Development/Acquisition Implementation	
X 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:

What is NHS?

The Environmental Protection Agency (EPA) owns, operates, and manages the National Hosting Service (NHS) to provide web and application hosting (WAH) services to EPA for a large variety of applications which support the EPA mission. The NHS supports large-scale data processing and provides a national data repository for Agency environmental and administrative systems. NHS provides dedicated, shared, and virtualized computing resources running multiple various operating systems (OS). Virtualized computing is accomplished by utilizing hardware that is supported by the VMware's hypervisor for virtual machines and provides a computing platform for the Linux and Microsoft (MS) Windows server operating systems. Dedicated and additional shared computing configurations are provided by the NHS supporting various UNIX operating systems and (MS) Windows operating systems. The supported (MS) Windows operating systems are Windows 2003

and 2008. The supported UNIX operating systems include Sun Solaris, IBM AIX, and Linux. The servers support a wide range of software including the Oracle database management system, Apache, SAS, iPlanet, Cold Fusion, Lotus Domino, Apache, and other application hosting software.

NHS does provide access to the cloud – but it's not a part of the cloud.

Who is NHS?

NHS user organizations include EPA program offices, regional offices and lab sites, states, universities, and the public. The NHS additionally provides special restricted access to entities external to EPA to meet the Agency's collaborative computing needs with a variety of cooperating organizations in government, industry, and academia. The organization responsible for the planning, design, operation, management, and maintenance of the EPA NHS is the OEI/OTOP/NCC, located in Research Triangle Park (RTP), North Carolina. Everyone can see the applications hosted at NHS depending on their role and the rules applied to each role for each individual system. Users can request tasks be performed by authorized NHS personnel – but no role of user at any level is able to modify NHS in any way.

NHS Assumptions

NHS is an empty container upon which IT Systems with their own IT Security Plans host data upon. NHS Systems hosted within the NHS Defined System Boundary may collect PII.

Application owners should assume that any security requirements associated with systems or functions not listed above are NOT addressed by the GSS security plan. The controls documented within this GSS security plan specifically exclude the unique security requirements of customer developed applications, application environments not managed by NCC, and customer managed authentication systems. For example, the scope of the controls within the security plan do not address the security requirements for customer developed or managed code or modules associated with:

1. continuous monitoring
2. custom application logging
3. application oriented training
4. the sensitivity analysis of customer content and data

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?

2 Title III of the E-Government Act of 2002, Federal Information Security Management Act (FISMA)
3 The Privacy Act of 1974, PL 93-579, as amended
4 The Freedom of Information Act, PL 93-502
5 The Federal Managers' Financial Integrity Act (FMFIA), PL 97-255
6 OMB Circular A-130, *Management of Federal Information Resources*
7 United States Code 44 U. S. C. 15 U. S. C.
8 OMB Circular A-123 Revised, *Management's Responsibility for Internal Control*, December 2004
9 OMB Circular A-127, *Financial Management Systems*, July 23, 1993
10 OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
11 FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
12 FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
13 NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
14 NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*

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. The SSP is dated 12/03/2019

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?

No. NHS is an onsite hosting facility, it is not hosted in the cloud.

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).

NHS Seeks to declare that although the NHS does not in itself collect PII, a subset of Applications deployed to NHS may or may not. NHS will mitigate all privacy controls for the Host Platform in the NHS Security Plan, however each system is required to maintain its own Privacy Threshold Analysis and if applicable for that specific application, a Privacy Impact Assessment or SORN per Agency standards.

The systems within NHS are comprised of publicly accessible servers (PA), production internal servers, and staging internal servers, which are all protected from direct Internet traffic by EPA managed firewalls. The public access servers primarily consist of UNIX and MS Windows servers that allow Hypertext Transfer Protocol (HTTP), Secure Sockets Layer (SSL), and File Transfer Protocol (FTP) limited access from registered Internet addresses. The production internal servers have Internet access restricted to pre-approved IP addresses and services. Internal staging servers are used for development and testing applications. All servers within the NHS can be accessed by IP addresses within the internal EPA IP domain network. Security perimeter zones are established between each of the groups of NHS resources as follows:

- Public Access (PA) – EPA servers that host publicly available web sites. The DMZ Firewall isolates them from the Internet.
- Staging and Production Internal Servers – Internal EPA servers sit behind the DMZ firewall and the Agency firewall which isolate them from the Internet.
- The Web Emergency Operations Center (WebEOC) and Central Data Exchange (CDX) environments are isolated from the internet and from internal EPA servers by the EPA managed firewalls. CDX and WebEOC are covered by separate SSPs.

The Micrososft Azure definition of PaaS is as follows: Platform as a service (PaaS) is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications. You purchase the resources you need from a cloud service provider on a pay-as-you-go basis and access them over a secure Internet connection.

https://azure.microsoft.com/en-us/overview/what-is-paas/

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

NHS provides dedicated, shared, and virtualized computing resources running multiple various operating systems (OS). Virtualized computing is accomplished by utilizing hardware that is supported by the VMware's hypervisor for virtual machines and provides a computing platform for the Linux and Microsoft (MS) Windows server operating systems. The sources of information do not come from NHS directly– NHS is simply a platform to host applications upon. The sub systems residing within NHS are the source of the information and individually decide on how their information is collected. The source of privacy information is collected at the application level, not the network or server level. Again, the source of privacy data is each application hosted at NHS.

NHS will mitigate all privacy controls for the Host Platform in the NHS Security Plan, however each system is required to maintain its own Privacy Threshold Analysis and if

applicable for that specific application, a Privacy Impact Assessment per Agency standards. The source of PII comes from the subsystems hosted under the defined within NHS system boundary.

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

NHS does not use information from outside sources. NHS is a collection of servers, routers, network appliances and infrastructure equipment. It's not a database that uses data from another source, and it's not an application which would reference any external information. Its only purpose is to host agency applications. The scope of which these applications use data is defined within the security plan of that specific application hosted at NHS.

2.4 Discuss how accuracy of the data is ensured.

Each application hosted at NHS is responsible for the accuracy of its data. NHS is responsible for backing up data which is hosted there, but the accuracy of that data is only measurable by Application Specific System Owner(s) or System Points of Contact (POC's).

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:

What each IT Application collects with regards to privacy data affects it's characterization Collecting more information than is required to identify submitted data properly could occur.

Mitigation:

NHS hosted IT Applications or subsystems need to document the source of information and collection accordingly. Annually as part of the certification and accreditation process, collection of Privacy data is examined and properly documented.

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?

NHS privileges to server and network administration accounts observe the use of "least privilege". Access is granted based on roles and responsibilities must be approved and submitted by the supervisor or system owner. The request form lists the reasons for the requests. All system default accounts are automatically removed as per specific Operating System Security Checklists and Standard Configuration Documents.

User access to NHS resources is via web browser or application-specific client software using TCP/IP-based networking protocols. Access to NHS equipment must be made from within the NHS defined system boundaries.

NHS maintains user accounts in accordance with account policy and procedure guidelines.
• Following Agency standards, it is recommended that users run with a minimal set of permissions whenever possible.
• Standard user accounts have limited permissions on the system but are able to perform most common day-to-day tasks.
• Administrator user accounts have full permissions on the computer, but users can run with minimal permissions for most tasks.
• You can enable the Guest account for use by individuals who might need to access the system occasionally.
• Custom Account maintenance is provided on an as-needed basis and requires justification for custom criteria.
• Local Users and Groups are maintained for use with standard security configuration, including group membership.

The systems within NHS are comprised of publicly accessible servers (PA), production internal servers, and staging internal servers, which are all protected from direct Internet traffic by EPA managed firewalls. The public access servers primarily consist of UNIX and MS Windows servers that allow Hypertext Transfer Protocol (HTTP), Secure Sockets Layer (SSL), and File Transfer Protocol (FTP) limited access from registered Internet addresses. The production internal servers have Internet access restricted to pre-approved IP addresses and services. Internal staging servers are used for development and testing applications. All servers within the NHS can be accessed by IP addresses within the internal EPA IP domain network. Security perimeter zones are established between each of the groups of NHS resources as follows:

- Public Access (PA) – EPA servers that host publicly available web sites. The DMZ Firewall isolates them from the Internet.
- Staging and Production Internal Servers – Internal EPA servers sit behind the DMZ firewall and the Agency firewall which isolate them from the Internet.
- The Web Emergency Operations Center (WebEOC) and Central Data Exchange (CDX) environments are isolated from the internet and from internal EPA servers by the EPA managed firewalls. CDX and WebEOC are covered by separate SSPs.

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

The NHS System Security Plan (SSP).

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

Access to an application and access to the host platform are not inter-related by design. No application has access privileges to server hardware, or operating system.

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?

NHS account administrators do not create temporary accounts and notification emails are sent when individuals terminate their employment and accounts are locked or removed as specified. NHS follows all Agency standard practices for account management, and follows the Agency SAISO Guidance separation checklist for account deletion from the LDAP services.

24.104 Contract clauses.
When the design, development, or operation of a system records on individuals is required to accomplish an
agency function, the contracting officer shall insert the following clauses in solicitations and contracts:
(a) The clause at 52.224-I, Privacy Act Notification.
(b) The clause at 52.22 violation 4-2, Privacy Act.

52.224-1 Privacy Act Notification.
As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

Privacy Act Notificaiton (APR 1984)
The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(End of clause)

52.224-2 Privacy Act.
As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

PRIVACY ACT (APR 1984)

(a) The Contractor agrees to—

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies—

(i) The systems of records; and
(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.
(c)(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

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.

Auditable events are described as the ingestion of records into the repository and the scheduled disposition of records from the system based on pre-defined records retention schedules. These events are audited on a weekly basis by reports generated from the NHS

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 NHS system administrator and the EPA NHS Program Management Office.
Documentation:

EPA's auditing policies are documented in:
• EPA Order 2195A1. (See the note in the Security Control, AU-1)
• Agency Network Security Policy OTOP 200.03
• Systems Engineering Monitoring and Log Review Procedures
• Standard Configuration Documents
• Monthly security Scan Results
• Support of IG Criminal Investigations
• UNIX and Windows Security Checklists
• Systems Engineering Policy on Security Scanning.
• Support of IG Criminal Investigations

Specific to NHS:

EPA Records Schedule 0742
http://intranet.epa.gov/records/schedule/final/0742.html

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:

Individual application owners at NHS are required to follow agency standard record management. NHS does not assume ownership of individual IT Application data.

Mitigation:

The Privacy Impact Assessment document as well as mitigation of NHS privacy controls are both conducted on a yearly bases and are a part of the annual certification process.

Information Security Privacy Procedures: CIO Transmittal # 15-008 details the mitigation of Privacy controls which includes references to record retention. Risk analysis for specific privacy act controls include:

1. DM-2 Data Retention and Disposal:

- Retain each collection of PII for the period identified in NARA record retention schedules to fulfill the purpose(s) identified in the notice or as required by law;

2. IP-1 Consent

- Provide means, where feasible and appropriate, for individuals to authorize the collection, use,

maintenance, and sharing of PII prior to its collection. Provide appropriate means for individuals to understand the consequences of the decision to decline the collection, use, dissemination and retention of PII;

3. Definition of Information Owners (IO)

in coordination with the Director of OIC; Retain collection of PII for timelines identified in NARA record retention schedules to fulfill the purpose(s) identified in the notice or as required by law;

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.

NHS Does not share any information with outside entities.

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

NHS Does not externally share any information with outside entities.

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?

NHS Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements. For connecting systems that have the same SIO, an ISA is not required. Rather, the interface characteristics between the connecting information systems shall be described in the System Security Plans (SSP) for the respective systems.

1. An approved Interagency Agreement (IA) or Memorandum of Understanding / Agreement (MOU/A) signed by a SIO is implemented with the ISA.

2. NHS Routes connections through the agency's Trusted Internet Connection (TIC) solution or equivalent approved by the SAISO and adhere to requirements promulgated in TIC directives.

3. The SO submit an interconnection request to the EPA's National Computer Center (NCC) Director. The request shall include the following:

a. Type of connection to be established,
b. Connection requirements,
c. Key personnel to help coordinate the planning efforts of the system interconnection,
d. Duration of the interconnection, and
e. Point of contact for the external organization requesting the interconnection.

4. The Director, NCC reviews and approves or rejects the request and sends a copy of the acceptance or rejection letter to the SO, SIO, ISO, and the point of contact for the external organization requesting the connection. If rejected, the letter shall include the rejection reason(s) and corrective actions needed for acceptance.

4.4 Does the agreement place limitations on re-dissemination?

NHS Does not share any information. It is simply a platform to host applications on.

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:

None. NHS Does not share any information. It is simply a platform to host applications on.

Mitigation:

None. NHS Does not share any information. It is simply a platform to host applications on. NHS avoids this IT security weakness by requiring individual IT Application owners to assume responsibility for application specific information.

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 in accordance with stated practices in this PIA (Section 6.1)?

NHS is a host platform, Each System Owner is responsible for the privacy information of that particular system.

Annually, a review of risk is performed prior to Authorization of usage

This system has a system banner which displays to users system policies before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

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

EPA's National Privacy Program ensures compliance with statutory and regulatory requirements for collecting and safeguarding Personally Identifiable Information. Annually, all EPA employees are required to take Privacy training.

EPA's implementation of the Privacy Act can be found at:

https://www.epa.gov/privacy

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Training for accountability of privacy data is a requirement of all EPA employees. This annual process is controlled outside the boundaries of NHS. On an annual basis, IT system specific data is examined during the ATO process.

Mitigation:

Privacy training is required annually, not completing that results in loss of user account access.

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.

NHS Does not use information. It is a platform to host applications.

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 dentifier(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 retrieval of information from NHS is defined within the security plan for each application for which data is being retrieved. NHS provides a platform to host applications on, and each application could use different methods of retrieving information which are specific to that application. Retrieving data is application specific – thus the definition of hot data is retrieved is specified in each applications SSP. Individual IT Applications as part of their annual certification and accreditation process require examination of the use of PII by the Privacy Office. A Privacy Impact Assessment would contain each personal identifier if required.

NHS is a hosting platform. None of the NHS components or services are accessed by the public. The responsibility of NHS stops at the hardware and operating system. Each System owner facilitates access of individual IT systems thru the use of a user interface. Individual IT Application user interfaces are not contained within the NHS System boundary. Any modification to a system requires the use of the Application Development Checklist (ADC) process. Approvals are required before access to NHS is granted to maintain the IT application.

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Currently NHS does not have a SORN.

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 risk that data in the individual application could be used for an unauthorised purpose.

Mitigation:

The use of Privacy data for each IT application requires the approval of the Privacy office, and that approval is examined yearly as part of the annual Application CMA process for Authorization to Operate (ATO). Application specific controls are in place to help protect data align with Incident Response procedures which help to protect, detect, and investigate incidents.

*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.

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:

Mitigation:

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?

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

8.3 How does the system notify individuals about the procedures for correcting their information?

8.4 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:

Mitigation: