

# 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](https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx)

<b>System Name:</b> Enterprise Wide Area Network (EWAN)	
<b>Preparer:</b> Lemont Phelps/ David Szczepanski/John Kahanek	<b>Office:</b> OEI/OITO/NSOD
<b>Date:</b> 01/26/2021	<b>Phone:</b> 919-541-7599
<b>Reason for Submittal:</b> New PIA ___ Revised PIA ___ Annual Review <u> X </u> Rescindment ___	
<b>This system is in the following life cycle stage(s):</b>	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input checked="" type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
<b>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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u></b>	
<b>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</u></b>	

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

The Network Access Control (NAC) system is a sub-component of the Enterprise Wide Area Network (EWAN). The NAC solution allows the EPA to authenticate, authorize and audit, non-EPA users and devices to the wireless network. The NAC system collects the following publicly available company data:

- Company Email Address
- Company Phone Number
- Company Name

## **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?**

This plan was developed in response to the requirements of the following laws and regulations:

- 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.
- The Title of the E-Government Act of 2002 - Federal Information Security Management Act (FISMA) – Public Law 107-347: A security plan must be developed and practiced throughout all life cycles of the agency's information systems.
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources: A System Security Plan (SSP) is to be developed and documented for each GSS and Major Application (MA) consistent with guidance issued by the National Institute of Standards and Technology (NIST).
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems: This document defines standards for the security categorization of information and information systems. System security categorization must be included in SSPs.
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems: This document contains information regarding specifications for minimum security control requirements for federal information and information systems. Minimum security controls must be documented in SSPs.
- NIST Special Publication (SP) 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems: The minimum standards for an SSP are provided in this NIST document.
- NIST SP 800-53, Revision 4, Recommended Security Controls for Federal Information Systems and Organizations: This document contains a list of security controls that are to be implemented into federal information systems based on their FIPS 199 categorization. This document is used in conjunction with FIPS 200 to define minimum security controls, which must be documented in SSPs.
  - EPA Information Security Planning Policy. A system security plan shall be developed for each system cited on the EPA Inventory of Major Information Systems, including major applications and general support systems.

### **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, EWAN currently has an ATO that will expire on **December 16, 2022**.

**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 - No systems external to the Network Access Control systems have access to the data contained within the NAC ISE database. The ISE (Identity Services Engine) database is part of the platform. It has nothing to do with AT&T. ISE is the platform, NAC is a service provided by the platform.

## **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).**

The base publicly available company contact information is collected for accountability when access is granted for the Guest Internet.

- Company Email Address
- Company Phone Number
- Company Name

The point of contact (PoC) is the Sponsor, whom is required to be an EPA federal employee, requesting publicly available company guest access on behalf of their guest.

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

The point of contact (PoC) is the Sponsor, whom is required to be an EPA federal employee, requesting publicly available company guest access on behalf their guest.

The base publicly available company contact information is collected for accountability when access is granted for the Guest Internet.

- Company Email Address
- Company Phone Number
- Company Name

The more technical information follows. The NAC system stores the above listed data in a CISCO proprietary platform, ISE (Identity Services Engine) that is maintained by the EPA, which runs on a Linux platform. All data is stored in an internal Structured Query Language (SQL) Net database that uses an embedded FIPS-2 validated cryptographic module (Certificate #1643). The data is gathered by regional hosts who submit Remedy tickets on behalf of the guest. Either the EPA call center or the NSO group enters the information into the NAC ISE subsystem in order to create credentials that will allow non-EPA users to access Internet resources only.

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

Yes, the commercial source data is collected through the PoC/Sponsor. This data will be used to create temporary wireless user accounts for access to the Internet ONLY.

The point of contact (PoC) is the Sponsor, whom is required to be an EPA federal employee, requesting publicly available company guest access on behalf of their guest.

### **2.4 Discuss how accuracy of the data is ensured.**

The accuracy is ensured because the point of contact (PoC) is the Sponsor, whom is required to be an EPA federal employee, requesting publicly available company guest access on behalf of their guest.

The base publicly available company contact information is collected for accountability when access is granted for the Guest Internet.

- Company Email Address
- Company Phone Number
- Company Name

### **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:**

Data elements collected are as follows.

1. Company Email Address
  - a. Risk that email address may contain the user's name.

2. Company Phone Number
  - a. No known risk as the company phone number is publicly listed.
3. Company Name
  - a. No known risk as the company name is publicly listed.

**Mitigation:**

1. Company Email Address
  - a. Information is stored in the secure ISE database. At the 90 day mark the information is purged from the system.
2. Company Phone Number
  - a. No mitigation as company phone number is publicly listed.
3. Company Name
  - a. No mitigation as company name is publicly listed.

**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, Only Systems Administrators, to include EPA security professionals with privileged access to the NAC devices and the EPA Government sponsors who will be provisioning the accounts.

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

Only Systems Administrators, to include EPA security professionals with privileged access to the NAC devices and the EPA Government sponsors who will be provisioning the accounts. Access to the system is achieved via role-based access levels. Only system administrators or EPA security professionals with privileged accounts have access to the system. Those individuals have been trained on the use of the system and have been approved by NSOD. The procedure is part of the EPA NSO Equipment and Application Access Management SOP.

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

Yes, the NAC/ISE subsystem has assigned roles and responsibilities within the EWAN 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?**

Federal employees as well as contractors will have access. Yes, the appropriate FAR clauses are included in the contract.

**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.**

The data is kept for a duration of 90 days. All account details will be purged thereafter. The data provides the Systems Administrators and EPA security personnel with the ability to have visibility and traceability of the account provisioning process. Additionally, it allows for the identification of individuals with accounts at any given time, should a security incident occur that requires forensic investigation.

EPA schedule number 404-1012d. Located at <http://intranet.epa.gov/records/schedule/final/1012.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.*

The 90 day retention period is standard and follows agency policy

**Privacy Risk:**

Minimal risk as the data will reside solely in the NAC ISE database until purged at the 90 day mark.

**Mitigation:**

Only Systems Administrators, to include EPA security professionals with privileged access to the NAC devices and the EPA Government sponsors who will be provisioning the accounts. Access to the system is achieved via role-based access levels. Additionally, encryption of the database prevents direct access. Between role based access and encryption, the NAC ISE database publicly available company data is secure. Also, purging occurs every 90 days.

**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 – No external or internal agencies, state or local government will have access to the data contained within the NAC ISE database

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

N/A – No external or internal agencies, state or local government will have access to the data contained within the NAC ISE database.

**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?**

N/A – No external or internal agencies, state or local government will have access to the data contained within the NAC ISE database.

**4.4 Does the agreement place limitations on re-dissemination?**

N/A – No external or internal agencies, state or local government will have access to the data contained within the NAC ISE database.

**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 – No external or internal agencies, state or local government will have access to the data contained within the NAC ISE database.

**Mitigation:**

None

## **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?**

There are SOPs regulating the use of information gathered and used in the NAC/ISE sub-system for the sole purpose of creating guest wireless credentials for non-EPA employees including EPA contractors.

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

All EPA users are required to take mandatory Annual EPA Information Security and Privacy training per CIO 2151.0 – Privacy Policy and CIO 2150.3 EPA Information Security Policy.

### **5.3 Privacy Impact Analysis: Related to Auditing and Accountability**

#### **Privacy Risk:**

None. Auditing and accountability occurs through NAC ISE logging.

#### **Mitigation:**

None. Auditing and accountability occurs through NAC ISE logging.

## **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.**

The NAC/ISE subsystem uses the information for the purpose of creating user credentials so that the user may access Internet resources provided freely by the agency. The information allows for the identification of individuals with accounts at any given time, should a security incident occur that requires forensic investigation.

The publicly available company information collected for accountability includes

- Company Email Address
- Company Phone Number
- Company Name

### **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.)*

The NAC subsystem is not designed for information to be retrieved by the user. Only Systems Administrators, to include EPA security professionals with privileged access to the NAC devices and the EPA Government sponsors have access to the information. The company email address will be used as the identifier.

The point of contact (PoC) is the Sponsor, whom is required to be an EPA federal employee, requesting publicly available company guest access on behalf of their guest.

The base publicly available company contact information is collected for accountability



when access is granted for the Guest Internet.

- Company Email Address
- Company Phone Number
- Company Name

**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 base publicly available company contact information is collected by the EPA Government Sponsor directly from the guest for accountability when access is granted for Guest Internet use after which the information is purged after 90 days, thus the individual's information is not maintained in the Systems of Records.

**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.*

SOPs regulating system use and agency security policies are in place to ensure the information is handled as outlined in this

**Privacy Risk:**

Minimal risk as only Systems Administrators, to include EPA security professionals with privileged access to the NAC devices and the EPA Government sponsors who will be provisioning the accounts.

**Mitigation:**

All EPA users are required to take mandatory Annual EPA Privacy training per CIO 2151.0 – Privacy Policy and CIO 2150.3 EPA Information Security Policy.

**\*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 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:**