Privacy Impact Assessment

For

Non-GFE for Remote Access

Date:

May 26, 2015

Point of Contact and Author:

Michael Gray
michael.gray@ed.gov

System Owner:

Allen Hill
allen.hill@ed.gov

Office of the Chief Information Officer (OCIO)

U.S. Department of Education

1. System Information.

Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions. Indicate whether the system is new or existing and whether or not the PIA is new or being updated from a previous version; specify whether the system is "agency" or "contractor."

The Network Access Control (NAC) is technology implemented to monitor the end points connecting to the network and enforce compliance to Department policies. By implementing this technology, the Department will be able to identify and prevent unauthorized and unsafe devices from accessing its trusted network, to have situational awareness of devices connected to the network, and enforce endpoint security compliance policies. NAC validates the security posture of endpoints against standard policies prior to granting access to the Department's trusted networks.

Endpoints are any system or device that connects to the Department's network and communicates with other entities over the network infrastructure such as servers, desktop computers, laptops, printers, and internet protocol (IP) phones. Endpoints can vary in hardware types, operating systems, and applications, and can be used within Department-managed facilities, data centers, employees' homes, and other remote places outside the Department's control. Endpoints can be government furnished equipment (GFE) or non-GFE.

2. Legal Authority.

Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

Privacy Act of 1974 5 U.S.C. § 552a (e)(10). Agencies are required to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

3. Characterization of the Information.

What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

NAC collects and maintains information about users' network and computer, but it does not collect or maintain Personally Identifiable Information (PII). In the course of monitoring the endpoints and determining whether the device should be granted access to the ED Network, the system will have access to employees' names and work contact information (phone number, email address), as well as information about the device being used to access the ED Network, such as operating system being used, switch and port information, and account information.

The system will be hosted on the EDUCATE Network. The EDUCATE PIA can be found here: http://www2.ed.gov/notices/pia/educate_102809.pdf

The source of the information collected on GFE on the EDUCATE network will be Active Directory.

4. Why is the information collected?

How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

The NAC accesses the data for the purpose of validating the security posture of all endpoints against standard policies prior to granting access to the Department's trusted networks, thus preventing compromised endpoints from accessing the trusted network and potentially compromising sensitive Department information. The potential privacy risk is that the system will have the ability to access endpoint information, including that of non-government furnished equipment. The risks are mitigated by accessing the least amount of information necessary to accomplish the objective. Additionally, the information that is collected will only be stored on the NAC appliance for no more than 4 days (96 hours). This technology is being implemented to improve the security posture of the ED Network. This technology will actually improve privacy risks, as it will reduce the risk of data breach risk associated with security vulnerabilities. In this case, the benefit of improving the overall security posture, outweighs the slight risk to personal privacy.

5. Social Security Number (SSN).

If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

This technology does not collect, view, or access Social Security Numbers.

6. Uses of the Information.

What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

The information accessed as part of the NAC solution will be used by the EDSOC/EDCIRC to validate the security posture of all supported endpoints against standard policies as they connect to the Department's trusted network. When a policy violation is detected on the endpoint, the technology prevents compromised endpoints from accessing the trusted network and potentially compromising sensitive Department information.

7. Internal Sharing and Disclosure.

With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

EDSOC/EDCIRC will share this information with the OCIO/Network Services Team, the Office of the Inspector General, and law enforcement, as required.

8. External Sharing and Disclosure.

With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

The information will not be shared outside of the Department.

9. Notice.

Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

A banner informing ED employees of the NAC technology will be displayed when employees log onto the system. Additionally, the Department or OCIO will be publishing notices on Ed-Notebook, and other ED communication methods.

In addition to the above, all employees are required to take annual Security Awareness Training. This training includes an explanation regarding the monitoring of governmental systems and devices and specifically notes that these systems and devices are monitored – and that no reasonable expectation of privacy should be assumed. Users grant consent when signing the rules of behavior for network access, and are prompted by a warning banner each time they access the network.

10. Web Addresses.

List the web addresses (known or planned) that have a Privacy Notice.

There will be no public facing web address for this system; therefore a privacy notice is not required.

11. Security.

What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

Since the NAC technology is part of the EDUCATE infrastructure security boundary, all NAC's administrative, technical and physical security safeguards are covered by the current EDUCATE C&A and Authority To Operate (ATO).

12. Privacy Act System of Records.

Is the information within the system retrieved by personal identifier? If so, is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

A system of record notice is not needed because any information collected is not retrieved by name or personal identifier. Therefore, a system of record as defined by the Privacy Act is not being created and the reporting requirements of OMB Circular A-130 do not apply.

13. Records Retention and Disposition.

Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

Records are maintained and disposed of in accordance with NARA’s General Records Schedules 20 and 24.