Privacy Impact Assessment

For

McAfee Data Loss Prevention System (DLP)

Date:

May 11, 2015

Point of Contact:

Jason Hawkins
jason.hawkins@ed.gov

System Owner:

Allen Hill
allen.hill@ed.gov

Author:

Adam Avila
adam.avila@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."

McAfee Data Loss Prevention (DLP) solution is designed to analyze, identify, alert and prevent the unintentional or deliberate exfiltration of unprotected sensitive data from the Department's network. It operates at two (2) layers:

1. Host based and network based, and
2. From Endpoint Client to Internet Gateway appliances.

McAfee DLP can locate and identify sensitive data stored in:

- Databases
- Network shared drives
- Application data repositories

It will also identify and block the transmission of sensitive data via:

- Web traffic
- SMTP (web-mail)
- Social media sites
- Blogs

It can control copy & paste, printing, and the use of, and transfer of, sensitive data to external media.

The McAfee DLP solution is being implemented as part of the EDUCATE Security system boundary.

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?

The elements of Personally Identifiable Information (PII) being collected and maintained are:

- Names
- Social security numbers (SSN)
- Dates of birth
- Home addresses

- Home telephone numbers
- Personal email addresses
- Financial Information

The sources from which this information derives are all EDUCATE systems, security personnel and/or any contractors assisting them with the express intent of preventing and reporting on possible PII exfiltration attempts.

The EDUCATE PIA can be found here: http://www2.ed.gov/notices/pia/educate_102809.pdf

The information is collected via the DLP discover, monitor, and web gateway appliances that operate at two (2) layers:

1) Host based and network based, and
2) From Endpoint Client to Internet Gateway appliances.

McAfee DLP can locate and identify sensitive data stored in:

- Databases
- Network shared drives
- Application data repositories

It will also identify and block the transmission of sensitive data via:

- Web traffic
- SMTP (web-mail)
- Social media sites
- Blogs

It can control copy & paste, printing, and the use of, and transfer of, sensitive data to external media.

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.

McAfee DLP collects PII during the course of scanning Department systems in an effort to determine whether or not a file has violated a defined policy -- and to provide an appropriate means of identifying Department personnel (or any contractors assisting them) who own the violating file, i.e., an email with PII data can actually be identified and blocked from leaving the network. This transaction can be used as evidence for an internal investigation, audit trail or criminal or civil prosecution. The system exists to reduce the data breach risk associated with the exposure of unencrypted sensitive data.

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.

The SSN is one PII element that the DLP can scan for and identify throughout the EDUCATE network, as described above. For example, it is Department policy that SSNs may not be emailed unencrypted. The DLP can scan the Department's email system for SSNs, and block emails containing unencrypted SSNs from leaving the network. Because such an email is a policy violation and its discovery is a

function of the tool, the SSN is captured during the course of scanning Department systems. The transmission/transaction can be collected and used as evidence for an internal investigation, audit trail, or criminal or civil prosecution. Because the purpose of the DLP is to detect unauthorized disclosure and use of PII, specifically SSNs, there is no alternative that could be used.

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.

Department systems security personnel (and any contractors assisting them) use the data collected in the tool on a need to know basis in an effort to determine if the violating file is legitimate or actually a false positive -- and to determine the appropriate owner of the violating file. Determining the file owner is critical for properly remediating the violation and for following up with appropriate training.

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?

The information will be shared with Department's Security Operations Center/Computer Incident Response Capability (EDSOC/EDCIRC), Privacy Safeguards Division, the Privacy Incident Response Team, Human Capitol and Client Services, Office of the Inspector General, and law enforcement, if 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 be shared in accordance with Departmental Guidelines, the Department Privacy Office and with Privacy Act, 5 U.S.C. 552a (c) in order to comply with Office of the Inspector General or Law Enforcement Investigations as required.

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?

The Department or OCIO will be publishing notices in accordance with the Communication Plan via office flyers, email notifications, Web Ed-Notebook, and other 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?

The evidence folder is a secured shared drive that can be accessed by DLP managers. Access controls are in place (username/password required) and only DLP administrators have access. The data captured and written to the evidence folder is encrypted. A Standard Operating Procedure (SOP) will also be written for system access requests, as well as use and operation.

The System is compliant with both National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA) requirements. Per the requirements of FISMA, security assessment and authorization requirements are being met for the EDUCATE Security system boundary that the DLP solution will be a part of. The assessment and authorization process is an audit of policies, procedures, controls, and contingency planning, and is required to be completed for all federal government IT systems. All relevant policies, procedures and guidelines, including NIST Special Publication 800-53, are being followed to ensure the security of the system and the information it contains.

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 records notice is not needed because the 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.