

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/26/2016

OPDIV:

OS

Name:

Splunk

PIA Unique Identifier:

P-1669045-575729

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Development

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The purpose of the Splunk system is to provide information on one screen to show information like which computers have a virus or which computers have Ransomware. This information can then be used for researching, analyzing, and responding to security incidents within HHS.

Describe the type of information the system will collect, maintain (store), or share.

Splunk will collect threat feeds and logs from Information Technology Infrastructure Operations (ITIO) supported assets and aggregate this data to provide a secure way to search, analyze and visualize potential alerts within the environment.

Splunk acts as central log aggregator and correlation engine for alerts, system, and event logs from Information Technology Infrastructure Operations (ITIO) supported assets including servers, end-user endpoints, and network and security devices. In addition, Splunk receives cyber threat intelligence feeds from iSIGHT Partners, FireEye, and other sources. Splunk will aggregate this data into usable alerts for the Security Operations Center (SOC) Analysts and Incident Response Team

(IRT) to investigate as needed.

Critical alerts will be delivered to the IRT via email. Alerts are customizable according to the query supplied to the tool. For IRT's purposes, alert queries will be constructed to detect indications of compromise (i.e., indicators for possible ransom-ware infections).

Splunk will aggregate this data into usable alerts for the Incident Response Team (IRT) to investigate and respond to as needed. Alerts will be delivered to the IRT as email alerts. For IRT's purposes, alert queries will be constructed to detect indications of incidents (i.e., indicators for possible ransom-ware infections).

A unique Splunk account and user credentials are required to access the alert and the additional identifying details. The end user's HHS Active Directory (AD) user name used to log onto their device will be captured in the system event logs. Our Security Analysts will then be able to identify the end user if the account used is a unique identifier and not a generic account (i.e., not using the user's first and last name).

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

Splunk is a tool designed to assist security analysts in collecting, analyzing, and acting upon logs generated by technology infrastructure, security systems and business applications. Splunk will support OS by serving as the Security Information Event Management (SIEM) tool for the OS IRT. This system will aggregate logs and threat intelligence feeds from ITIO supported systems. Splunk will also collect logs from servers that have been configured to send logs to it. These logs will be correlated in a database. This data will be stored on dedicated machines for 6 months to 1 year depending on storage capacity.

Type of information collected in the logs will contain information provided from security and encryption tools installed on all GFE laptops. Collected PII is limited to Full Name and HHS Email for HHS employees (Fed/Contractor). PII collected is from is forwarded from the OS email systems and Enterprise Network Management (ENMS) systems. Information included in the logs include: IP address, last Check Point Endpoint System (CPES) check-in date, and encryption status.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

E-Mail Address

User Credentials: email address and password

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The user names within the logs will be used to assist the IRT in identifying the users of the devices in cases of potential incidents. If an alert requires escalation beyond initial review, OS IRT will use the PII (user name) to identify the user and coordinate next steps with the appropriate teams-HHS ITIO Service Desk & HHS ITIO server teams-as needed.

Describe the secondary uses for which the PII will be used.

There are no immediate plans for PII use beyond the use cases above. Possible secondary uses of the PII may include trend analysis of past incidents to determine infection patterns. Examples of infection patterns may include repeatedly targeted users. This may yield to information about links in successful exploits (i.e., user's with patch status or browser plug-ins). Direct lookups for research will be through the alert date/time/signature or the Risk Vision/Remedy number created as a result of that investigation.

Identify legal authorities governing information use and disclosure specific to the system and program.

42 US Code, The Public Health and Welfare. This is the Title of the US Code that implements HHS and provides it with the legal authority to operate.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

Not applicable

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

There is no direct process in place to notify users that their PII will be collected for use in Splunk. PII used within the system is limited to name and email address only. Splunk is an aggregator tool. Software that will provide the PII (Full Name/Email) is software that is commonly on all HHS ITIO Government Furnished Equipment (GFE) laptops-Checkpoint/Endpoint Security (CPES) is an example of one such service. Users will receive notifications from the HHS ITIO Service Desk through email and software installation.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

The warning on every user's computer when they log into the HHS domain explains that you are agreeing to be monitored while using the computer and the network. So if you click on OK and continue to log in, it means you accept the conditions of the warning. Therefore if you log into the computer or the domain, everything you do is being monitored and is in the purview of the government. And since you log in with your user name, that information is part of what is being monitored. This is why there is no option to opt-out-of the collection or use of PII, unless you choose not to log into the government computer or the domain. The PII being collected is limited to name and email address for federal employees and supporting contractors.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

If we must disclose any PII data, the HHS ITIO Service Desk will notify the user via an email or by phone.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

In the event an employee believes that their PII has been inappropriately obtained, used, or disclosed, the employee may contact the HHS Computer Security Incident Response Center, HHS ITIO Service Desk, or OS Incident Response Team directly to report an incident via email. User's are provided the CSIRC's email address via the Annual Security Awareness trainings. The HHS ITIO Service Desk can also provide each email address to any users upon request.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

The logs in Splunk are coming from Email system and Active Directory where the system owners already have processes in place for data integrity, availability, accuracy, and relevancy. Splunk simply gets a copy of this information. And as these logs are in transit to the Splunk servers, the data on the wire, per ITIO standards, is protected. When the data reaches the Splunk servers, only the Splunk administrators can access this information. And since Splunk servers are within the ENMS system boundary, all the certification and accreditation controls and processes for ENMS are inherited by the Splunk servers and administrators for the Splunk servers. Therefore the data on Splunk certainly has integrity, availability, accuracy, and relevancy.

Identify who will have access to the PII in the system and the reason why they require access.

Administrators:

OS IRT members only. The tool will be used exclusively by IRT for incident identification, confirmation, and response. The contractors in OS IRT are those hired per the ITIO contract.

These administrators have gone through the HHS hiring process for the level of clearance that is appropriate for the work that they perform. These contractors were hired by ITIO to specifically do this work which ITIO deemed them qualified for. These contractors have HHS email addresses and access to the HHS network because they have gone through the rigid process per the ITIO contract to allow them such access to the HHS network. These contractors have gone through Splunk training to be administrators of Splunk.

Contractors:

Contractor access to the tool is limited to OS IRT's direct contractor support as system administrators.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Access to the Splunk system is restricted to OS IRT members only. Processes for new users include Splunk training and approval from the IR Lead before access is granted.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Role based access control exists for Splunk Administrators only. Access to the tool will be restricted to OS IRT.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All OS IRT Splunk users have received HHS Annual Privacy Training, Annual Security Awareness Training, ISSO training, and have reviewed of the Rules of Behavior Policy.

Describe training system users receive (above and beyond general security and privacy awareness training).

All OS IRT Splunk Administrators and Power Users have received training and certifications via classes provided by the vendor (Splunk).

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

We adhere to OS Security Policies to ensure the confidentiality, integrity, and availability of the PII data. This includes encryption standard, role-based access control, and chain of custody processes. PII retention is kept with the remainder of search-able for 6 months to 1 year depending on storage capacity.

National Archives & Record Administration (NARA) record retention follows:

IT Security schedule 817-4 for Incident Response Unclassified Systems. Record retention is for 1 year after cut off (N1-64-08-12, item 27)

System Engineering: Schedule 820 with destruction 5 years after cut-off (N1-64-08-12, item 33) and Data Management schedules 821-1 and 821-2.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Only designated personnel will have accounts to Splunk system but access control will be implemented based on user's role. Any PII data will be stored on Splunk servers and secured in an ITIO data center, which has additional physical controls and Closed-Circuit Television (CCTV) monitoring. Splunk account management will be monitored for irregular activity. Splunk will inherit all of ENMS's common controls, technical controls, and physical controls.

