

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/14/2014

OPDIV:

OS

Name:

Malware Virtualization Compartmentalization

PIA Unique Identifier:

P-7988940-281745

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Initiation

Is this a FISMA-Reportable system?

No

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.**

This system provides malware compartmentalization capabilities. Malware is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Invincea and Bromium are endpoint security tools that will be piloted enterprise wide. This pilot program will cover separate installations of both Bromium and Invincea Management Servers at each of the following Operational Divisions:

- CSO- Cyber Security Operations
- CDC- Center for Disease Control
- CMS- Centers for Medicare & Medicaid Services
- OIG- Office of Inspector General
- NIH- National Institutes of Health
- FDA- Food and Drug Administration

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

Log Data
Malware and Threat Data
User activities in relation to malware

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

Management Server collecting endpoint information on user machines. System will generate log data and malware and threat analysis data, permanently for the duration of the pilot.

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

Yes

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

Name
malware related web activities

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

Employees

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

Primary purpose of PII being used is for forensic investigation of malware. For user authentication its use will be the same as any information collected by firewalls and proxies such as IP addresses, ports and protocols. Its use is solely for incident attribution and tracking to resolution.

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

Secondary uses for use of PII will be for research into the pilot products.

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

Governing legal authority is FISMA, 44 U.S.C. 3541

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.**Identify the sources of PII in the system.****Directly from an individual about whom the information pertains****Government Sources**

Within OpDiv
Other HHS OpDiv

Non-Governmental Sources**Identify the OMB information collection approval number and expiration date****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.

All systems with the software installed will be subject to the standard system use notification at log on.

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

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.

Security tool installed on the system to monitor system activities.

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

Users are all federal IT users who agreed to data collection as part of their federal IT Rules of Behavior.

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.

Users are all federal IT users who agreed to data collection as part of their federal IT Rules of Behavior.

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

During this limited pilot there is no plan or process for further review.

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

Review of security logs

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

Administrators, managers responsible for network operations, will be able to access PII, users will not.

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.

There are no further restrictions. Administrators have access to all security log information within the system. The system only records user activities with regards to malware activity.

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 users have participated in system demo's for awareness and training purposes.

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

N/A

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

No

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

The system will be decommissioned at the end of the pilot, all information will be destroyed.
Estimated end of pilot date: June 9, 2014

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

Only system administrators can log into the system as well as protected by network boundary.