US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/20/2016

OPDIV:

OIG

Name:

CyberRange

PIA Unique Identifier:

P-3891963-583319

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

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 is to support OIG cyber assessment training as well as support cyber threat intelligence research. It is also purposed to be used as a platform from which the OIG can execute testing of HHS and Operating Division (OpDIV) systems.

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

OIG does not control the original collection of PII from the HHS and OpDiv systems. Hence the system-related information collected by CyberRange during testing or assessments could potentially contain a vast range of PII, including Social Security Numbers, Financial Information, Medical Notes, etc. Information includes system-related information collected during tests or assessments. This could include any type of information on the target computer(s). Once testing is completed, all sensitive data and the infrastructure on which the data was temporarily stored is securely destroyed.

Information that may be temporarily collected could include:
User names

IP/MAC address
Passwords
User account IDs
Social Security Number
Name
Driver’s License Number
Mother’s Maiden Name
E-Mail Address
Phone numbers
Medical Notes
Certificates
Education Records
Military Status
Foreign Activities
Taxpayer ID
Date of Birth
Photographic Identifiers
Biometric Identifiers
Vehicle Identifiers
Mailing Address
Medical Records Number
Financial Account Info
Legal Documents
Devices Identifiers
Employment Status
Passport Number

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

This is a general support system which collects and temporarily stores data as a result of scans and testing of HHS systems. OIG does not control the original collection of PII from the HHS and OpDiv systems. Hence the system-related information collected by CyberRange during testing or assessments could potentially contain a vast range of PII. This could include any type of information on the target computer(s). Any information collected and/or temporarily stored is solely for purposes of security testing. In any testing scenario it is impossible to know which type(s) of information may be collected. Once testing is completed, all sensitive data and the infrastructure on which the data was temporarily stored is securely destroyed.

User credentials for all system users are collected and maintained in order to perform logging and audits and for purposes of non-repudiation.

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

Yes

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

Social Security Number

Date of Birth

Name

Photographic Identifiers

Driver's License Number

Biometric Identifiers

Mother's Maiden Name

Vehicle Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Certificates

Legal Documents

Education Records

Device Identifiers

Military Status

Employment Status

Foreign Activities

Passport Number

Taxpayer ID

User credentials

IP/MAC addresses

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

PII could be used to identify a particular system on the network (e.g. MAC or IP address) in the context of test results. User credentials are collected to grant and manage access to the system.

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

N/A

Describe the function of the SSN.

If SSN is collected/accessed it is as a by-product of main system function it is not used by CyberRange. All data is deleted at the close of an assessment.

Cite the legal authority to use the SSN.

Inspector General Act of 1978, 5 U.S.C. App. 3, as amended.

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

Inspector General Act of 1978, 5 U.S.C. App. 3, as amended.

Privacy Act of 1974

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Foreign

Other

Non-Governmental Sources

Public

Commercial Data Broker

Media/Internet

Private Sector

Other

Identify the OMB information collection approval number and expiration date

N/A

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

Within HHS. We will share the data that was accessed with the HHS OPDIV or business owner of system, unless they request that we do not.

Describe any agreements in place that authorizes the information sharing or disclosure.

We execute a Rules of Engagement document with the HHS OPDIV prior to conducting the testing which describes the rules governing the test, notification of vulnerabilities, and how sensitive data, if collected, will be shared with OpDIV and protected while maintained in CyberRange system.

Describe the procedures for accounting for disclosures.

Disclosures back to the OpDIV will be documented in reports and outcomes documents.

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

As part of the audit function of the OIG the penetration testing is not announced.

The banners on federal information systems provide notice that the information in the system is not private. Any information that CyberRange accesses was initially collected by another OpDIV or contractor working on behalf of the OpDIV and the collection notification requirements accrue to that initial collection. Collection of user IDs, credentials and passwords is defined by the Rules of Engagement (RoE) for the test event.

The RoE indicate that the OIG will notify the HHS OPDIV point of contact at the point in which any test results in the exposure of Personally Identifiable Information (PII) or Classified information.

Some of the PII collected by the system may be considered "mandatory" under the provisions of legal authorities applying to the OpDIV that originally performed the collection. For more information about these authorities refer to the appropriate PIA for the information in question.

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.

OIG does not control the original collection of PII and any PII collected and temporarily stored by the system is collected incidentally as a result of testing efforts and subsequently deleted. User credentials are required to unambiguously identify user activity and enable non-repudiation.

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

No information is permanently stored in the system so a system change would not impact any data. Provision of user credentials is considered consent to the collection and management of that data. System owner/administrators will notify users of major changes to the system if they are determined to impact the collection and maintenance of user credentials.

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.

Complaints of this nature should be directed to the initial collecting entity. Users of the system can direct concerns to system administrators, who will escalate to the system owner as appropriate.

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

PII is not contained in the system for any period of time. User credentials are protected by administrative, technical and procedural processes/safeguards to ensure integrity, availability, accuracy and relevancy. Only administrators with a demonstrated need for access to user credentials may access this PII to manage the system. All system access is logged to ensure that user credentials and other PII are protected from inappropriate access. User accounts are reviewed quarterly and any inaccuracies corrected at that time or upon notification from a user of an inaccuracy (sent to system administrators). All PII collected is considered relevant due to the purpose of the collection (system testing) but is not used, shared or otherwise manipulated in any way that would imperil the data integrity. Availability is ensured through contractual means (service level agreements) and system backups.

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

Users:

To perform system functions.

Administrators:

To perform system functions and administer user accounts.

Contractors:

Direct Contractors to perform system functions and maintenance.

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

PII temporarily stored in the system will be accessed only to share with OpDIV being tested. CyberRange users do not access PII for any other reason.

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 controls based on the minimum information necessary to carry out the user tasks.

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.

Security and Awareness training and training on safeguarding PII is completed annually by OIG employees and direct contractors using the system.

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

CyberRange users will be given role-based training.

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.

All data in the system is securely destroyed at the end of a test event. No PII in the system is created, used, or integrated into any record generated during the audit activity.

The audit activity is covered by:
OIG DAA-0468-2013-0010 (and -0002) - Temporary files are destroyed 8 years after cutoff (end of fiscal year in which audit was closed); Permanent records are transferred to NARA 5 years after cutoff.

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

PII is secured via the following sets of controls:
Administrative controls: Access is provided based on a demonstrated need to know, appropriate job responsibilities.

Technical controls: User Identification, Passwords, Firewalls, Virtual Private Network (VPN) solutions, Intrusion Detection Systems (IDS), Common Access Cards (CAC), Smart Cards, Biometrics, Public Key Infrastructure (PKI)

Physical Controls: Guards, Identification Badges, Key Cards, Closed Circuit TV (CCTV) and alarm systems.

Note: web address is a hyperlink.