US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/17/2025

OPDIV:

NIH

Name:

NIH Enterprise CSO Red Team Infrastructure

PIA Unique Identifier:

P-2466241-281224

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

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)?

Yes

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

Describe the purpose of the system.

Cyber Security Operations (CSO) Red Team Infrastructure constitutes a set of systems used during CSO Red Team cyber operation engagements, in order to effectively test the security of information technology (IT) systems at the NIH, and to simulate real world adversary activity in an IT environment.

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

The data stored on these systems typically include NIH system metadata information such as username, hostname, and information protocol (IP) addresses. However, by nature of performing Red Team operations to demonstrate impact, there may be a scenario where identifying, and exfiltrating (removing) sensitive data may be required. Therefore, these systems could, for a short period of time, store any category of personally identifiable information (PII). The user's machine could potentially house any of the following:

Social Security Number (SSN)

Name

Drivers License Number (DL Number)
Mother Maiden Name
E-Mail Address
Phone Numbers
Medical Notes
Certificates
Education Records
Military Status
Foreign Activities
Taxpayer Identification (ID)
Date of Birth (DoB)
Photographic Identifiers
Biometric Identifiers
Vehicle Identifiers
Mailing Address
Medical Records Number (MRN)
Financial Account Info
Legal Documents
Device Identifiers
Employment Status
Passport Number

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented. The purpose of the IAM is to authenticate and authorize all users and computers in a Windows domain type network, assigning and enforcing information security policies for all computers and installing or updating software. The IAM collects unique user credentials and stores them in an encrypted format. The IAM is an essential service which facilitates and governs network access to various resources.

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

CSO Red Team Infrastructure constitutes the set of primarily used to perform CSO Red Team activities. This includes multiple Linux servers that run the Cobalt Strike Command and Control (C2) framework, and the Brute Ratel C2 framework. This system will be used during CSO Red Team cyber operation engagements, in order to effectively test the security of systems at the NIH, and to simulate real world adversary activity.

The data stored on these systems will typically include NIH system metadata information such as username, hostname, and IP addresses. However, by nature of performing red team operations to demonstrate impact, there may be a scenario where identifying, and exfiltrating sensitive data may be required. Therefore, these systems could for a short period of time store any category of PII data. The user's machine could potentially house any of the following:
SSN
Name
DL Number
Mother Maiden Name
E-Mail Address
Phone Numbers
Medical Notes
Certificates
Education Records

Military Status
Foreign Activities
Taxpayer ID
DoB
Photographic Identifiers
Biometric Identifiers
Vehicle Identifiers
Mailing Address
MRN
Financial Account Info
Legal Documents
Device Identifiers
Employment Status
Passport Number

Those requiring access to this system log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

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
Username, hostname and IP 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?
10,000-49,999

For what primary purpose is the PII used?
Incidental data can be gathered as a by-product of collecting and exfiltrating data on a compromised user workstation.

Describe the secondary uses for which the PII will be used.
None

Identify legal authorities governing information use and disclosure specific to the system and program.
44 US.C § 3101 & § 3102
42 U.S. Code § 281

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
Online
Government Sources
Within the DOC
Non-Government Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date
Not applicable

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.
NIH Rules of Behavior and warning banners are displayed on NIH logon screens to access NIH systems. Users are required to read and accept these notices to obtain access.

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.
Sensitive data is collected at rest and in motion in order to protect it. Opting out is not applicable.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.
The NIH Rules of Behavior and Warning Banners displayed on logon screens for NIH systems would be updated.

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.

Individuals can contact the NIH IT Service Desk or NIH Privacy Office at: privacy@mail.nih.gov

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 stored temporarily and identified as such. It is stored as long as an engagement is active. At the end of the engagement, a report is provided and a redacted sample of PII captured is provided to demonstrate the impact of the breach/vulnerability.

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

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

CSO Red Team follows NIH policy to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

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.

CSO Red Team follows NIH policy to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

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.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security and privacy awareness training.

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

All users of the system are provided with system training via Skype/WebEx.

Administrators receive vendor training and hold industry security certifications.

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.

08-220 - Personally identifiable information extract logs. Destroy when business use ceases (DAA-GRS-2013-0007-0013).

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

Administrative Controls: PII is stored in the vendor Oracle database. Data is encrypted before the data is written to the database. Communication between the main console, scanner servers, endpoint management servers and endpoints are encrypted. Access to the console requires two factor authentication via smart card and personal identification number (PIN). The system is part of the Information Security (INFOSEC) General Support system (GSS) and inherits the physical controls from that parent system.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.

Physical Controls: The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.