# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

06/16/2016

### OPDIV:

OS

### Name:

ThreatConnect

**PIA Unique Identifier:**

P-8648617-499925

**The subject of this PIA is which of the following?**

Major Application

**Identify the Enterprise Performance Lifecycle Phase of the system.**

Planning

**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)?**

Yes

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

**Describe the purpose of the system.**

The Healthcare Threat Operations Center - Threat Intelligence Platform (HTOC-TIP) is a web-based solution based on CyberSquared's Threat Connect threat intelligence platform. The platform combines multiple analytical capabilities such as threat intelligence collection and management, threat analysis and collaboration. This solution provides a means for threat analysts from disparate federal agencies to share cyber threat information effortlessly and efficiently. The system collects PII about the analysts at those federal agencies who are granted access to the system, in order to administer their log-in privileges and monitor their system usage. When users post information in the collaboration portal they will be publicly attributed to their posts. If the user decides to collaborate with other users, their name is provided with their contribution.

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

The Stored Data data includes the following:
Threat-Actor and Threat related data (Non-PII)
Indicators of Compromise (IOC) (registry keys, IP addresses, domains, etc.. ) and related information usually associated with malware and actor campaigns. (Non-PII).

Log Data stored will include the following:
User Actions
Admin Actions
System Events
System Errors

All PII related data collected is name and business address for HHS employees, direct contractors and Space and Naval Warfare Systems Command & Veterans Affairs employees. Only government assigned email addresses and full name will be stored by the system. Passwords are not stored, a salted hash is stored in its place. All users require a government assigned email address plus a chosen password that meets complexity requirements to login to the system.
Salted hashes will not be shared.
Salted Hash - In cryptography, a salt is random data that is used as an additional input to a one-way function that "hashes" a password or passphrase. The salt portion is an extra series of numbers or letters added to the password before it is hashed making even easy passwords difficult to crack.

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

Web based system used to collect threat-actor and threat related information to share and collaborate amongst authorized government entities. Indicators of Compromise (IOC) (registry keys, IP addresses, domains, etc.. ) and related information usually associated with malware and actor campaigns will be stored within the system. All Non-PII related information will be stored indefinitely until IOC's are exonerated or no longer relevant. All PII related information will be stored according to applicable HHS policies. Audits will be performed to remove stale user account records.

**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

HHS User Credentials (email address and salted hash)

Business e-mail addresses

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

Employees

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

**How many individuals' PII is in the system?**

<100

**For what primary purpose is the PII used?**

The primary purpose of PII being used is to login the user at the prompt. This PII will identify the user of the system and actions/contributions made to the system.

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

N/A

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

Governing legal authority is FISMA, 44 U.S.C. 3544

**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.**

09-90-0777 Facility & Resource Access Ctrl Recs

**Identify the sources of PII in the system.**

Email

**Government Sources**

Within OpDiv

Other HHS OpDiv

Other Federal Entities

**Identify the OMB information collection approval number and expiration date**

NA - submissions are not in a standard format.

**Is the PII shared with other organizations?**

Yes

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

**Within HHS**

Any OpDiv

**Other Federal Agencies**

Space and Naval Warfare Systems Command & Veterans Affairs

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

Collected PII will be accessible to other Business Partners (Federal Agencies) during the usage of the tool as a collaboration medium. Memorandums of Understanding have been signed between all Federal Agencies using this tool.

**Describe the procedures for accounting for disclosures.**

N/A

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

No system collection point is given to the user as the user is requesting access to the system via email.

**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.**

PII required to access the system. If a user wishes to opt-out of PII collection a Threat Connect administrator can remove the user account.

**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 users who agreed to provide PII to be able to utilize the system. An email will be generated to all affected users if there are changes on how their PII is handled or used. An email is sent to request access and within the email is the source email address and name of the individual requesting access is then utilized to provide access.

**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.**

The user can contact designated Threat Connect and/or Computer Security Incident Response Center (CSIRC) administrators to rectify or process any issues that may occur.

**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 certification and accreditation requires periodic reviews of all government systems to achieve an authority to operate.

Several controls are in place to support the Confidentiality-Integrity-Availability of PII within the system.
Confidentiality - Hyper Text Transport Protocol Secure, Transport Layer Security , Encryption, Access Control Lists
Integrity - Transport Layer Security, Cyclical Redundancy Checks, Checksums, Role Based Access Control, Hashing
Availability - Redundant links ,Relational DataBase Management Systems, Backups

System Administrators will audit the system and remove accounts that have not been used after 60 days. Auditing and log records retention will be set to 3 months to comply with HHS policy.

Periodic review will occur in compliance with the following NIST and HHS guidelines:

NIST FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems
NIST FIPS Publication 200, Minimum Security Requirement for Federal Information and Information Systems
NIST Special Publication 800-37 Revision 1, Information Security
NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers
NIST 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information

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

**Users:**
Users can potentially see other user's posts in the collaboration process.

**Administrators:**
To setup accounts/Administrate accounts

**Contractors:**
Users can potentially see other user's posts in the collaboration process.

**Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.**
Role based access control- Only administrators can access user accounts. Administrators are setup as to be able to view the information associated with accounts that are created within the system. Roles are setup to only view and access information needed. Users can view the names of others that have submitted the posts in the collaboration portion.

**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- Only administrators can access user accounts. Administrators are setup as to be able to view the information associated with accounts that are created within the system. Users are setup to only information provided and potentially the names of others that have submitted the post.

**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 will complete the mandatory training, Privacy Security Awareness Training.

**Describe training system users receive (above and beyond general security and privacy awareness training).**
Not Applicable

**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.**

User Credentials retention schedule: General Records Schedule (GRS) 3.2. Item 010, Disposition Authority: DAA-GRS-2013-0006-0001. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

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

Only authorized administrators can view noted PII. System firewall and roles only allow for specific subset of users to access. Subset of users are only those that allowed through the firewall via a static Internet Protocol address. The IP address is owned by the user's organization. All other IP addresses are denied access. All servers and information processing equipment is maintained in a locked and secure area. All users are given an account for logical control. Role-based access control is used to further define account access. Administrative controls include security training provided to all federal employees.