

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

06/29/2016

**OPDIV:**

OS

**Name:**

Automated Indicator Sharing

**PIA Unique Identifier:**

P-5125855-907270

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

Minor Application (child)

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

Implementation

**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.**

The Automated Indicator Sharing (AIS) system enhances Cybersecurity information sharing among federal agencies. These cyber threat indicators and defensive measures are shared consistent with the need to protect information systems from cybersecurity threats, mitigate cybersecurity threats, and comply with any other applicable provisions of law authorized by the Cybersecurity Information Sharing Act of 2015 (CISA) in a manner that ensures appropriate incorporation of privacy, civil liberties, and other compliance protections.

The system receives threat and cybersecurity data in a text-based markup language, stores this data in its database, and redistributes this data to servers within each Operating Division's enclave across HHS.

Much of the information within an indicator is centered on an observable fact about the cyber threat. For example, a cyber threat indicator has a variety of observable characteristics: a malicious email, Internet protocol (IP) addresses, file hashes, domain names, uniform resource locators (URLs), malware files, and malware artifacts (attributes about a file).

The system will also store user credential information (name, email address) for the purposes of authentication. Users, administrators, and/or direct contractors will be authenticated with these credentials.

The Automated Indicator Sharing (AIS) system consists of three feeds: (1) Automated Indicator Sharing, (2) Federal Government (FedGov) and (3) Cyber Information Sharing and Collaboration Program (CISCP). The AIS feeds consists of bi-directional, real-time sharing of cyber threat indicators among federal departments and agencies, and the private sector. The FedGov feed consists of bi-directional, real-time sharing of cyber threat indicators only among federal departments and agencies.

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

Much of the information within an indicator is centered on an observable fact about the cyber threat. For example, a cyber threat indicator has a variety of observable characteristics: a malicious email, internet protocol (IP) addresses, file hashes, domain names, uniform resource locators (URLs), malware files, and malware artifacts (attributes about a file).

The system will also store user credential information (name, email address) for the purposes of authentication. Users, administrators, and/or direct contractors will be authenticated with these credentials.

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

The Automated Indicator Sharing system enhances Cybersecurity information sharing among federal agencies. These cyber threat indicators and defensive measures are shared consistent with the need to protect information systems from cybersecurity threats, mitigate cybersecurity threats, and comply with any other applicable provisions of law authorized by the Cybersecurity Information Sharing Act of 2015 (CISA) in a manner that ensures appropriate incorporation of privacy, civil liberties, and other compliance protections.

Cyber Threat Indicator and Defensive Measure data that could be collected through the Automated Indicator Sharing profile, including: Automated Indicator Sharing Organization Information (Organization Name, Sector, Location), Descriptions about the indicator, Descriptions of methods for defeating cybersecurity threats or security vulnerabilities, Observed facts about a cyber threat, or "Observables" (Email messages, IP Addresses, URLs, Hashes, Files, usernames, etc.) or Information or descriptors about observables.

If a submitter includes PII that the Department of Homeland Security (DHS) determines is not directly related to the cybersecurity threat, the Department of Homeland Security will remove the PII from the cyber indicator or defensive measure prior to dissemination. This data is intended and formatted for machine-to-machine exchange.

The system will also store user credential information (name, email address) for the purposes of authentication. Users, administrators, and/or direct contractors will be authenticated with these credentials. These credentials are also used to assign role-based access to data within the system.

The goal of the AIS initiative is for the HHS' Operating System (OS) to achieve real-time sharing of cyber threat indicators from the DHS's National Cybersecurity and Communications Integration Center (NCCIC). The HHS OS is enabled through the NCCIC to (1) receive indicators from the private sector and other non-federal entities; (2) remove unnecessary personally identifiable information; and (3) disseminate the indicators, as appropriate, to other federal departments and agencies and the private sector.

**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

**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?**

Controlling system access

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

Not Applicable

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

5 USC 301, Departmental regulations

**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

**Government Sources**

Within OpDiv

Other HHS OpDiv

**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.**

No notice is provided because the extent of PII collected is the data required to request an account.

**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.**

To opt-out, the user would decline access to the system by not providing their name or email address.

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

Users will be emailed at the provided email address.

**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 order to resolve an individual's concerns on the use of their PII, they may contact HHS CSIRC (Computer Security Incident Response Center) via email, at [csirc@hhs.gov](mailto:csirc@hhs.gov). Users should identify and describe their concerns, and they will be addressed.

**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 data collected is used for authentication purposes. Periodic reviews are not generally performed.

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

**Administrators:**

Administrators have access to usernames and email addresses for the purpose of user rights management.

**Contractors:**

Direct contractors, acting in an administrative role.

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

Role-based access control is used to ensure sufficient, but not excessive, access is maintained to user data. Administrative accounts are limited to the number necessary for ongoing operations of the system.

**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.**

Technical controls limit the visibility of user accounts to those with Administrative roles assigned.

**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.**

Annual HHS Information Systems Security Awareness Training and Annual HHS Privacy 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.**

GRS 24, section 6: Retention of user access database, containing usernames and passwords.

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

Administrative: Role based access, individual accounts

Technical: Encryption, automatic logoff

Physical: Facility access controls, system backups