Privacy Impact Assessment

for

CyberSentry

DHS Reference No. DHS/CISA/PIA-037

January 25, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has developed the voluntary CyberSentry program to enhance the cyber resilience of organizations that own or operate critical infrastructure. CyberSentry uses sensors to monitor the Information Technology and Operational Technology networks of a participating Critical Infrastructure (CI) partner for cybersecurity threats. CISA is conducting this Privacy Impact Assessment (PIA) because CyberSentry's network monitoring capabilities may create the potential for disclosure of personally identifiable information (PII).

Overview

Under the Homeland Security Act of 2002,[1] CISA is responsible for providing timely technical assistance, risk management support, and incident response capabilities, upon request, to federal and non-federal entities, including members of the 16 critical infrastructure sectors.[2] The assets, systems, and networks belonging to those sectors are considered so vital that their incapacitation or destruction would have a debilitating effect on national security, national economic security, national public health or safety, or a combination thereof.

Under the Homeland Security Act of 2002,[3] CISA is responsible for providing timely technical assistance, risk management support, and incident response capabilities, upon request, to federal and non-federal entities, including members of the 16 critical infrastructure sectors. The CISA Cybersecurity Division (CSD) operates the voluntary CyberSentry program to enhance the detection of cybersecurity threats to organizations that own or operate critical infrastructure. Within these critical infrastructure sectors, many components that were once operated by human beings are now managed, monitored, and controlled by computing systems, also known as Operational Technology (OT). These OT assets are increasingly Internet-accessible due to factors such as the growth in remote operations and monitoring, accommodation of a decentralized workforce, and the expansion of outsourcing of key skill areas such as instrumentation and control, OT asset management/maintenance, and, in some cases, process operations and maintenance.

CISA CSD operates CyberSentry out of its Threat Hunting Branch (TH). TH proactively hunts for malicious cyber activity, and also provides front-line response to cyber incidents, advises on mitigation strategies and assists critical infrastructure owners/operators to restore service. TH provides its CI partners recommendations for improving overall network and control systems

[1] *See* Title XXII of the Homeland Security Act of 2002 (6 U.S.C. §§ 651 - 674, esp. § 2209 of the Homeland Security Act (6 U.S.C. § 659(c)(6)).
[2] *See* Presidential Policy Directive-21 (PPD-21) of February 12, 2013 (Critical Infrastructure Security and Resilience).
[3] *See* Title XXII of the Homeland Security Act of 2002 (6 U.S.C. §§ 651 - 674, esp. § 2209 of the Homeland Security Act (6 U.S.C. § 659(c)(6)).

security. TH coordinates CyberSentry site assistance and technical evaluation activities through its Technical Engagement Network (TEN). The TEN's analytical capabilities include digital media analysis, host and network analysis, Industrial Control Systems analysis, and supporting discovery of on-site and remote cyber threats[4] and incidents.

CISA offers certain CI partners to which they have previously provided technical assistance the opportunity to participate in the CyberSentry program, based on a partner selection matrix. The matrix is currently being refined but contains criteria such as number of customers served, economic impact, market share, regional dominance, risk profile, technical profile, previous interactions with CISA, and regulated/non-regulated status. If the CI partner accepts the offer to deploy CyberSentry, it will sign a Memorandum of Agreement (MOA) with TH. The MOA contains a certification to CISA that CISA-reviewed and approved log-on banners are in place to obtain consent to monitoring. The MOA also establishes the means by which CISA and the CI partner will coordinate regarding equipment, software, and license acquisition as well as an initial set of validation tests for CISA to ensure proper configuration and optimal integration of CyberSentry within the partner's information technology (IT) network and its OT network.

CyberSentry hardware and software (when combined, referred to as the "stack") is installed and integrated within the CI partner's IT and OT networks via strategically placed network sensors.[5] Once deployed, the CyberSentry stack records all network traffic, including content of communications, and retains such data in limited access storage for as long as the stack's storage capacity will allow, while generating alerts based on signatures loading into the stack. At all times, CISA TH personnel can access network metadata collected by sensors placed on the OT network associated with network traffic between OT assets and the IT network. Similarly, CISA TH personnel can at all times access metadata collected by sensors placed on the IT network associated with network traffic between the IT network and the Internet. Metadata, often called data about data, covers non-content attributes such as sources, destinations, protocols, and other structural characteristics of the network traffic that can signal abnormal or suspicious activity.

Under the MOA between CISA and the CI partner, CISA may access all network traffic, including the content of communications, as stored within the CyberSentry stack to further analyze the origins of an alert[6] and/or evaluate the state of the network under the following conditions:

---

[4] Cyber threats can be defined as any identified efforts directed toward accessing, exfiltrating, manipulating, or impairing the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority. Information about cyber threats may be received from government, public, or private sources. Categories of cyber threats may include, for example: phishing, Internet Protocol (IP) spoofing, botnets, denials of service, distributed denials of service, man-in-the-middle attacks, or the insertion of other types of malware. *See* Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114–113, Division N, Title I, § 102, 129 Stat. 2936 (2015) (current version at 6 U.S.C. § 1501(5)(a)).

[5] Sensors collect data from networks in order to identify unusual or irregular network activity such as an adversary trying to exfiltrate data.

[6] An alert, in the context of CyberSentry capabilities, is when the program alerts a human analyst to suspected

- When CyberSentry generates an automated alert based on the comparison of network traffic against signatures[7] or deviation in baseline traffic;
- When either party identifies suspicious activity as having occurred on the network;
- When the infrastructure partner otherwise provides consent in a written communication (email is sufficient); or
- During the Annual Period of Advanced Analytic Development.[8]

CI partners must give individual users notice that their network interactions are subject to monitoring and an opportunity to consent. This is done through computer system log-on notices and consent banners that must be submitted by the CI partners to CISA for preapproval. These are provided for reference in Appendices A and B of this PIA.

While CyberSentry does not intentionally collect PII, it may be collected automatically within the network traffic capture as the program monitors the network traffic of the CI partner. CISA's own information handling practices require that when network traffic is analyzed in connection with a cyber threat, PII be removed or anonymized whenever it is not necessary to analyze or understand a cyber threat.

CISA may also issue alerts, advisories, bulletins, notices, or reports concerning threats detected through CyberSentry. These are also reviewed to determine whether they contain any PII, which may be included only if analytically relevant and necessary to understanding or responding to the cyber threat. In those instances, the Traffic Light Protocol (TLP)[9] information handling system is applicable; this protocol is a graduated system that marks, disseminates, and handles information based on its sensitivity.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The below authorities permit and define the collection of information by CyberSentry.

malicious activity.

[7] Signatures target known or suspected cyber threats by identifying specific characteristics of those threats.

[8] Each calendar year, there will be a 35-day period during which CISA will be permitted full data access to all the data traversing the IT and OT network of the CI partner. CISA will use this period of full data access for the purpose of developing the analytics it needs to generate automated alerts. For example, if a system on the network typically broadcasts "ABCDE" every five seconds, CISA would use this time to identify the "ABCDE" pattern and write a corresponding analytic to alert if that pattern or frequency changes.

[9] *See* U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), Traffic Light Protocol (TLP) Definitions and Usage, *available at* https://www.cisa.gov/tlp.

- *Homeland Security Act of 2002, as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018*, establishes and authorizes various functions for CISA's cybersecurity operations, including its role to, upon request, provide technical assistance, risk management support, and incident response capabilities to federal and non-federal entities related to cybersecurity risks and incidents.
- *Presidential Policy Directive (PPD) 21* advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. The directive instructs the federal government to work with critical infrastructure owners and operators and state, local, tribal and territorial (SLTT) governments to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Data collected through the CyberSentry sensors will not be filed, maintained, and retrieved by personal identifier. The data collected will be filed, maintained, and retrieved by security incident. Therefore, a Privacy Act System of Records Notice (SORN) is not required.

The Privacy Act does apply when general contact and other related information (such as username or a government-issued email address) is used to grant access to CyberSentry. The SORN titled, DHS General Information Technology Access Account Records Systems (GITAARS),[10] covers the collection of general contact and other related information used to grant access to employees, contractors, and other individuals to CyberSentry.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. CyberSentry is operated on the Technical Engagement Network (TEN) and is subject to that system's Authority to Operate (ATO). As part of the security authorization package for the TEN, a Security Plan was completed and the ATO was authorized in December 2019.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

DHS retains information obtained though CyberSentry only to protect the information and information systems of CI partners from cybersecurity risks. DHS retains information obtained through CyberSentry no longer than is reasonably necessary for the purpose of protecting

[10] *See* DHS/ALL-004 General Information Technology Access Account Records Systems (GITAARS), 77 Fed. Reg. 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

information and information systems from a cybersecurity risk. CyberSentry is part of the TEN and the TEN utilizes the National Cybersecurity Protection System (NCPS) records retention schedule. A records retention schedule for NCPS (Record Schedule #DAA-0563-2013-0008) was approved on January 12, 2015.[11]

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information is not being collected or solicited directly from the public; therefore, the Paperwork Reduction Act (PRA) is not applicable to the information collected by CyberSentry capabilities.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

CyberSentry collects network traffic, including metadata and the full content of network communications, and compares that information against signatures and baseline network traffic in order identify malicious traffic. When a signature for a known or suspected cyber threat triggers an alert or the data flow significantly skews from the baseline, a predetermined amount of associated traffic that is analytically relevant to the potential threat is reviewed by a CyberSentry analyst. This additional data could include IP addresses, ports, protocols, digital signatures, time stamps, direction/type of traffic, flags, and sensor name. CyberSentry does not intentionally collect specific information about individuals. However, PII may be unintentionally collected as part of the network traffic in the course of normal CyberSentry operations and may be reviewed if it is associated with a cyber threat. If the PII is identified as not relevant to the cyber threat, it is deleted.

General contact information such as name, title, agency name, email address, phone numbers, and other business-related information may be collected to grant employees, contractors, and other individuals CyberSentry access.

Through the MOA between the CI partner and CISA, the partner agrees that CISA may use the resulting analysis of information collected by CyberSentry to generate reports on topics including general computer network security trends and specific incidents, as well as indicators of

[11] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER DAA-0563-2013-0008, U.S. DEPARTMENT OF HOMELAND SECURITY, NATIONAL CYBERSECURITY PROTECTION SYSTEM (2015), DAA-0563-2013-0008, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0602/daa-0563-2013-0008_sf115.pdf.

anomalous or suspicious activity observed on the networks of those partners. Examples of indicators that may be shared include IP addresses, domain names, file names, and hash/digest values. Identification of a specific partner or individuals is anonymized in all reports that are transmitted outside of government. CISA may retain and share data that CISA has associated with a cybersecurity risk or suspected malicious activity with other entities in the U.S. Government with cybersecurity responsibilities. CISA may also share its analysis and conclusions within the U.S. Government, consistent with law.

2.2 What are the sources of the information and how is the information collected for the project?

CyberSentry uses strategically placed sensors across the IT and OT network of a CI partner to collect and log network traffic, including metadata, on to the stack. This collection occurs on a consistent basis and does not require any analyst intervention.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

CISA cybersecurity analysts use information from a range of sources, including commercial sources and publicly available data related to cybersecurity threats (e.g., open source internet searches, newspaper articles, operational uses of social media). This becomes part of the data that is used in creating signatures that trigger an alert during the monitoring process.

2.4 Discuss how accuracy of the data is ensured.

The signatures that are used to identify malicious network traffic are reviewed and approved by CISA in accordance with its written procedures and information handling practices. These procedures include validating the signatures to ensure they are active, useful, and within policy guidelines before being deployed. CISA also continuously monitors to confirm signature validation and verify expected results.

The CyberSentry capture and logging capabilities are not designed to manipulate or modify data. CyberSentry maintains exact copies of the network traffic as captured while traversing through the CI partner's IT or OT network. Therefore, data collected by a sensor is accurate because it is an exact copy of the data available.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that CyberSentry may collect PII from network traffic that is not necessary to understand or analyze a cyber threat.

Mitigation: This risk is mitigated. Full network traffic to include the content of communications may only be accessed by CyberSentry analysts and only in cases where traffic is related to a known or suspected cybersecurity threat or the partner has agreed to provide CyberSentry analysts access. If network traffic does not meet the criteria to trigger an alert or analyst query under the terms of the CyberSentry MOA, then the full network traffic is not viewed by CyberSentry analysts.

Additionally, any data that contains PII is managed in accordance with the appropriate CISA's information handling practices. All PII is reviewed prior to being included in any analytical products or other forms of dissemination. CISA written products, including alerts, advisories, bulletins, notices, and reports, are reviewed prior to dissemination to determine whether they contain any PII. Such information shall be included only when necessary to understand the product and to protect information systems from cybersecurity risks, mitigate cybersecurity risks, or respond to cyber incidents. In some cases, a product may include PII because that information is deemed analytically relevant and necessary to understanding the cyber threat. In those instances, CISA's information handling practices provide safeguards for the marking, dissemination, and handling of the information. If the PII is identified as not relevant, it is deleted.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Metadata, signatures, alerts, and portions of network traffic on the IT and OT networks of the CI partner are used to identify and respond to cybersecurity incidents and anomalies.

CISA may also share analysis and conclusions based on the incidents and anomalies in the form of a report and/or the sharing of indicators of malicious activity related to cybersecurity including but not limited to IP addresses, domain names, file names, and hash/digest values without disclosing where the information came from.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

CyberSentry is not configured or used to complete queries based on PII. Queries are limited to data and cyber incident information necessary to identify trends in cyber threat indicators and disparate data sets.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. While CyberSentry is part of the TEN, only CISA-authorized CyberSentry analysts with CyberSentry responsibilities will have access to the CyberSentry system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that PII inadvertently obtained via CyberSentry capabilities will be used or disclosed inappropriately.

Mitigation: This risk is mitigated. Access to the CI partner's network is limited to authorized users[12] assigned to the program. All CISA-authorized CyberSentry analysts are trained on both DHS and CISA specific procedures for handling and safeguarding PII. Those personnel receive privacy training upon being hired and are required to take annual refresher training. In addition, CISA maintains information handling practices for the identification of sensitive information and the proper handling and minimization of PII.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Notice is provided to CyberSentry program participants through their CISA-reviewed and approved computer system log-on consent banners or notices used to inform users and obtain their consent to CyberSentry monitoring and the terms and conditions of computer use. CI partners that deploy CyberSentry are required to provide to CISA for approval evidence that they have appropriate notices, banners, or other measures in place to provide individuals with notice that their network interactions are subject to monitoring and that users should have no expectation of privacy regarding any communications or information transiting, stored on, or traveling to or from the CI partner's information systems, including work-related use and personal use without exception.

Model language for log-on banners for computers and model language for a user agreement is provided to participating CI partners as part of the MOA with CISA. These are provided for reference in Appendices A and B of this PIA. In addition, this PIA also serves as notice of CyberSentry capabilities.

[12] The term "authorized users" in this document refers to authorized and trained federal employees, contractors, and other individuals that have been granted access to CyberSentry and its related components.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

All authorized users logging into a CI partner's network with CyberSentry capabilities are presented with an electronic notice or banner that notifies them that the computer systems are being monitored. These users can then decide if they wish to use the system and if so, decide what information they want to transmit over the computer systems.

Once a user accepts the electronic notice or banner (in most cases by clicking "OK" to proceed), the network traffic is subject to the computer security and related efforts of the CI partner, including in this case CyberSentry. This monitoring is in addition to any individual computer security programs the CI partner may have in place.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that a person may not be aware of or understand that network traffic may be collected by CyberSentry.

Mitigation: This risk is mitigated. CI partners that deploy CyberSentry must deploy CISA-reviewed and approved log-on consent banners that make clear disclosure of network traffic to governmental entities will occur and continued use of the network by the user represents consent to such monitoring and disclosure. Through these efforts, users provide their consent to the terms and conditions of computer use, including that their communications and data transmission are stored on the partner's network and that network traffic is subject to monitoring and disclosure for network security and other lawful government purposes.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

Data collected through CyberSentry capabilities is retained in accordance with the approved records retention schedule for NCPS (DAA-0563-2013-0008).[13] Non-network traffic data is retained for three years or until it is no longer needed for agency business, whichever is later. The network traffic metadata and content on communications related to an identified threat or indicator will be retained so newly discovered threat signatures can be compared against the archived data to determine if a newly understood Advanced Persistent Threat (APT) or similar activity can be seen in the archived data. Network traffic that is not associated with a cybersecurity threat is deleted on an on-going basis based on the storage capacity of the individual CyberSentry equipment operating at the critical infrastructure operator's facility.

[13] *See supra* note 10.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that PII may be retained beyond what is necessary to appropriately analyze or address a cybersecurity threat and may be exposed if there is a security breach.

Mitigation: This risk is mitigated. PII may be retained as part of a CI partner's network traffic captured by CyberSentry but is not accessed during the retention period unless it is determined to be related to a cyber threat. Network traffic is retained so that if new cyber threats are identified, the older metadata can be analyzed using newly created signatures.

CISA information handling practices provide the procedures for collection, processing, retention, and dissemination of PII. The practices also include proper data security procedures during the retention period. Because the only use CyberSentry makes of PII is in the context of investigating network traffic for cyber threats, concerns about diminished accuracy over time are not present.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

As part of its computer network security responsibilities, CISA generates reports on topics including general computer network security trends, specific incidents, and anomalous or suspicious activity observed on computer networks of its federal and non-federal partners. The identification of specific individuals or entities is generally anonymized in reports shared outside the U.S. Government. These reports are made available to DHS organizations and other federal Executive Departments and Agencies, through systems such as the US-CERT.gov secure website for their use in infrastructure protection and other computer network security related responsibilities. PII is only disseminated if sharing the actual PII is analytically relevant to understanding the cyber threat. If PII needs to be disseminated to stakeholders outside the U.S. Government, written approval must be obtained from CISA CSD leadership in advance of dissemination, in accordance with CISA information handling practices.

CISA also shares analysis, along with additional computer network security products, with its partners and constituents (federal departments and agencies; state, local, and tribal governments; industry; academia; the general public; and international partners) via US-CERT.gov.

Further, as a standard operating procedure, CISA notifies law enforcement or an intelligence entity of cyber incidents of relevance to the mission, primary jurisdiction or other applicable authorities for action.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

CyberSentry does not collect or retrieve information about identified individuals but rather security events that trigger an alert. Because CISA does not retrieve CyberSentry information by personal identifier, a SORN is not required.

The routine uses of general contact and other related information (such as username or a government-issued email address) used to grant access to CyberSentry are governed by the DHS/ALL-004 General Information Technology Access Account Records Systems SORN

In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records of information contained in these systems may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3).

6.3 Does the project place limitations on re-dissemination?

Cyber threat information resulting from CyberSentry monitoring is reviewed to determine if it contains PII and if so, that PII is only disseminated if sharing the actual PII is analytically relevant to understanding the cyber threat. If PII needs to be disseminated to stakeholders outside the U.S. Government, written approval must be obtained from CISA CSD leadership in advance of dissemination, in accordance with CISA information handling practices. Additionally, CISA typically restricts dissemination and re-dissemination of cyber threat information using the TLP.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

CISA provides cyber-related information to the public, federal departments and agencies, SLTT governments, and international entities through a variety of products, many of which are available on the US-CERT.cisa.gov website.

No reports disseminated via the US-CERT.cisa.gov website contain PII unrelated to a cyber threat. Each report is numbered and catalogued, and references exist in all products to tie back to a single incident or series of incidents that precipitated the product itself. If PII must be released, it is released in accordance with the Privacy Act of 1974,[14] appropriate CISA information handling practices, and with the authorization and/or written approval of CISA leadership.[15]

[14] 5 U.S.C. § 552a.
[15] Approval is not required when information about a specific person is believed to be fictitious, when the

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that PII obtained via CyberSentry capabilities will be shared inappropriately.

Mitigation: The risk is mitigated. Unauthorized disclosure is mitigated through various means, including encrypting the information and limiting access to the information. CISA has developed internal information handling practices governing the use of PII. All PII related to a cyber threat is reviewed and only shared if it is determined to be analytically relevant.

CISA information handling practices require that reports that contain PII be marked to identify the PII and if the report is modified for multiple audiences, each version is reviewed for appropriate markings. The practices include procedures for handling and limiting dissemination of particular types of PII. Information identifying sources and methods is required to be redacted from all CISA reports and products prior to dissemination.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

The only aspect of CyberSentry that is subject to access provisions of the Privacy Act is log-in/contact information covered under the GITAARS SORN. Individuals seeking access to any record containing information that is part of a DHS system of records may submit a Freedom of Information Act (FOIA) request to the DHS/CISA FOIA Officer. U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may file a Privacy Act (PA) request to access their information. Individuals may obtain instructions on how to submit a FOIA/Privacy Act request at https://www.dhs.gov/how-submit-foia-or-privacy-act-request-department-homeland-security. Please write to:

CISA FOIA Officer
245 Murray Lane SW
Washington, D.C. 20528-0380

Individuals may also make information inquiries to CISAFOIA@hq.dhs.gov.

The release of information is subject to standard FOIA exemptions and, given the nature of the cyber threat information contained in CyberSentry, CISA may not always permit individuals to gain access to their record(s).

information is publicly available, or when the release of such information is being coordinated with the person with whom it is associated.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals seeking to amend the accuracy of the content of a record containing information that is part of a DHS system of record may submit a FOIA or Privacy Act request to the DHS/CISA FOIA Officer. Individuals may obtain instructions on how to submit a FOIA/Privacy Act request at https://www.dhs.gov/how-submit-foia-or-privacy-act-request-department-homeland-security. Please write to:

CISA FOIA Officer
245 Murray Lane SW
Washington, D.C. 20528-0380

Individuals may also make information inquiries to CISAFOIA@hq.dhs.gov.

7.3 How does the project notify individuals about the procedures for correcting their information?

This PIA serves as notification to the public of proper avenues in place to contact the Department regarding information collections, including procedures for accessing and correcting information. The GITAARS SORN applicable to CyberSentry also provides notice of the redress procedures for this type of information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will want to seek redress for PII associated with a known or suspected cyber threat but are unable to do so.

Mitigation: This risk is mitigated. CISA has measures in place that allow individuals to request access to records of log-in/contact information. Additionally, this PIA and applicable GITAARS SORN provides notice for individuals seeking redress related to account log-in/contact records. These procedures are described in Sections 7.1, 7.2, and 7.3 above. Moreover, due to the nature of the CyberSentry system and the security risks it addresses, there is very little PII collected by the project.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CISA has developed information handling practices that govern the collection, handling, and dissemination of cybersecurity information. For CyberSentry specifically, CISA employs technical and manual mitigations and sanitization procedures that provide additional assurance that PII not directly related to a cybersecurity threat is removed from the CyberSentry stack.

Additionally, the MOAs between CISA and the CI partner also establish requirements and controls for accessing information on the CI partner's IT and OT network in a manner that is consistent with this PIA.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All DHS employees are required to complete annual Privacy Awareness Training. In addition, CISA CSD cybersecurity analysts (including CyberSentry analysts) are required to participate in periodic training on the procedures and practices for the handling of cybersecurity information. This training includes instructions on how to manage privacy risk when developing and deploying new signatures, analyzing network flow records, creating reports, and sharing incident information with partners.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

CyberSentry has a team of assigned analysts and support teams who are determined to have a need to know by TH and subject to relevant non-disclosure agreements as needed for access to the TEN. These users are granted special roles on the TEN to enable access to the CyberSentry enclave where access to the CI partner's alerting data is provided.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The MOAs developed between DHS and participating CI partners are based on an approved template that has been coordinated and approved by the program manager, system owner, CISA Office of the Chief Counsel, and the CISA Office of the Chief Privacy Officer. Agreements are reviewed periodically and updated when data usage, privacy policies, access procedures, or other conditions are identified. New uses of the information and new access to the system by organizations within DHS and outside are similarly reviewed by various stakeholders, including integrated program teams with approval vetted through upper management.

Contact Official

Mike Ray
CyberSentry Issue Coordinator
CISA/CSD/TH
michael.s.ray@cisa.dhs.gov

Responsible Official

Mark Bristow
Cyber Defense Coordination Branch Chief
CISA/CSD/TH

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

James V.M.L. Holzer
Acting Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A: Model Language For Log-On Banners For Computers

By clicking [ACCEPT] below you acknowledge and consent to the following:

All communications and data transiting, traveling to or from, or stored on this system will be monitored. You consent to the unrestricted monitoring, interception, recording, and searching of all communications and data transiting, traveling to or from, or stored on this system at any time and for any purpose by [XXX] and by any person or entity, including government entities, authorized by [XXX]. You also consent to the unrestricted disclosure of all communications and data transiting, traveling to or from, or stored on this system at any time and for any purpose to any person or entity, including government entities, authorized by [XXX]. You are acknowledging that you have no reasonable expectation of privacy regarding your use of this system. These acknowledgments and consents cover all use of the system, including work-related use and personal use without exception.

Appendix B: Model Language For User Agreement

By signing this document, you understand and consent to the following when you access XXX's information systems:

- You are accessing an information system that is provided for authorized use only;
- Unauthorized or improper use of the information system may result in disciplinary action, as well as civil and criminal penalties;
- XXX, acting directly or through its contractors or other authorized entities, including governmental entities, routinely monitors communications occurring on its information systems. You have no reasonable expectation of privacy regarding any communications or data transiting, stored on, or traveling to or from XXX information systems. At any time, authorized entities, including governmental entities, may for any lawful purpose monitor, intercept, search, and seize any communication or data transiting, stored, or traveling to or from XXX information systems;
- Any communications or data transiting, stored on, or traveling to or from XXX information systems will be monitored and may be disclosed or used for any lawful purpose; and
- These acknowledgments and consents cover all uses of XXX information systems, including work-related use and personal uses, without exception.

I understand and consent.

<<SIGNATURE BLOCK TO BE INSERTED LATER>>