Privacy Impact Assessment
for the

Automated Indicator Sharing (AIS)

DHS/NPPD/PIA-029(a)

March 16, 2016

Contact Point
Andy Ozment
Assistant Secretary
Office of Cybersecurity & Communications
National Protection and Programs Directorate
(703) 235-5999

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C) has developed an Automated Indicator Sharing (AIS) initiative to enable the timely exchange of cyber threat indicators and defensive measures among federal and non-federal entities. 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. Central to the AIS initiative and consistent with the requirements of CISA, the DHS National Cybersecurity and Communications Integration Center (NCCIC) serves as the centralized hub for exchanging cybersecurity threat information using a DHS-accredited infrastructure. NPPD is conducting this Privacy Impact Assessment (PIA) because personally identifiable information (PII) may be submitted as part of or accompanying a cyber threat indicator or defensive measure. This PIA updates and retires DHS/NPPD/PIA-029 Automated Indicator Sharing PIA, issued October 28, 2015.

Overview

The Department of Homeland Security (DHS) National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C), as authorized by the Cybersecurity Information Sharing Act of 2015 (CISA),[1] and further codified by Section 227 of the Homeland Security Act of 2002,[2] as amended by the Cybersecurity Act of 2015,[3] employs the Automated Indicator Sharing (AIS) initiative to enable federal[4] and non-federal[5] entities to share indicators of, and defensive measures for, cybersecurity threats.

The AIS initiative is an automated capability that receives, processes, and disseminates cyber threat indicators[6] and defensive measures[7] in real-time by enabling DHS's National

[1] Pub. L. No. 114-113, https://www.congress.gov/114/bills/hr2029/BILLS-114hr2029enr.pdf.
[2] 6 U.S.C. § 149.
[3] Pub. L. No. 114-113, https://www.congress.gov/114/bills/hr2029/BILLS-114hr2029enr.pdf.
[4] Federal entities, as defined by CISA, include any department or agency of the United States or any component of such department or agency. CISA further names "appropriate federal entities" required to receive cyber threat information under CISA. The appropriate federal entities include: Department of Commerce, Department of Defense, Department of Energy, Department of Homeland Security, Department of Justice, Department of Treasury, and the Office of the Director of National Intelligence.
[5] Non-federal entities, as defined by CISA, include any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof). Non-federal entities also include Information Sharing and Analysis Organizations (ISAOs), and by inclusion Information Sharing and Analysis Centers (ISACs), which are organizations engaged in information sharing related to cybersecurity risks and incidents. For more information about ISAOs, ISACs, or voluntary standards for standing up an ISAO, please visit: http://www.dhs.gov/isao.
[6] CISA defines a "cyber threat indicator" as information that is necessary to describe or identify: (A) malicious

Cybersecurity and Communications Integration Center (NCCIC) to (1) receive indicators from federal and non-federal entities; (2) remove personally identifiable information (PII)[8] and other sensitive information not directly related to the cybersecurity threat;[9] and (3) disseminate the cyber threat indicators and defensive measures, as appropriate, to other federal and non-federal entities.

The successful implementation of AIS will support federal and non-federal entities in addressing cybersecurity threats[10] to public health and safety, national security, and economic security while ensuring appropriate privacy, civil liberties, and other compliance protections.

Anticipated Phases of the AIS Initiative

Capabilities for the AIS initiative are being developed in phases in order to better leverage existing resources from within the Federal Government. This approach will allow DHS to deploy the AIS initiative while enhancing its capabilities over time. The anticipated phases are:

reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; (B) a method of defeating a security control or exploitation of a security vulnerability; (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability; (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (E) malicious cyber command and control; (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (H) any combination thereof.

[7] CISA defines a "defensive measure" as an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability--except those measures that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure or another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

[8] CISA utilizes the term "personal information" in establishing the requirement to remove any information not directly related to a cybersecurity threat that a participating entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual. However, since CISA does not explicitly define "personal information", DHS is using its definition of Personally Identifiable Information (PII), which it defines as: Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the United States.

[9] In addition to PII, sensitive information includes commercial, financial, and proprietary information of a non-federal entity, as identified or flagged by the non-federal entity.

[10] CISA defines a "cybersecurity threat" as an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system--except any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Pre-CISA

- **Initial Phase:** Develop and deploy a DHS system that can disseminate computer-readable cyber threat indicators to federal departments and agencies and limited private sector partners (described below) to supplement the existing mostly manual process.
- **Expanded Automation:** Develop and deploy DHS infrastructure that can receive, filter/sanitize, analyze, and disseminate cyber threat indicators from the private sector at large.

Post-CISA

- **Conform AIS to CISA:** Modify AIS to adhere to CISA's statutory requirements and the guidelines developed in support of those requirements. Retired DHS/NPPD/PIA-029 Automated Indicator Sharing PIA, issued October 28, 2015, which addressed previous states. This PIA reflects the post-CISA environment and will be updated as necessary to reflect subsequent phases.
- **Final Phase:** Fully automate DHS processes to receive and appropriately disseminate cyber threat indicators and defensive measures in a machine-readable format and finalize policies for filtering, receipt, retention, use, and sharing indicators, including regular compliance reviews.
- **Shared Services:** Implement a shared services capability that helps federal departments and agencies participate in automated cyber threat indicator and defensive measure sharing regardless of cybersecurity sophistication or resources.

AIS Participation

All federal and non-federal entities, as well as foreign governmental and foreign private sector entities,[11] are eligible to participate in the AIS initiative. During the early stages of AIS, however, participants will include only the appropriate federal entities as designated by CISA and select non-federal entities to ensure a stable rollout of AIS capabilities. All federal entities that participate in the initial phase of AIS are existing partners under the Enhance Shared Situational Awareness (ESSA)[12] Multilateral Information Sharing Agreement (MISA), which

[11] Foreign powers are excluded from the definition of non-Federal entity in CISA, and thus cannot benefit from CISA's protections. However, DHS operates AIS under not only CISA but also other authorities than CISA (see e.g., 6 U.S.C. § 148(c), (g)). Foreign powers may thus participate in AIS.

[12] Charter members of ESSA include the Defense Cyber Crime Center (DC3), Intelligence Community Security Coordination Center (IC-SCC), National Cybersecurity and Communications Integration Center (NCCIC), National Cyber Investigative Joint Task Force (NCIJTF), National Security Agency/Central Security Service (NSA/CSS) Threat Operation Center (NTOC), and United States Cyber Command (USCYBERCOM) Joint Operations Center (JOC). However, it should be noted that all government agencies will be allowed to participate in AIS upon signing the ESSA MISA. For more information on ESSA, please visit https://www.us-cert.gov/essa.

defines rules, guidelines, and policies for Government sharing of cyber information. To receive cybersecurity threat information through AIS, participating federal entities are required to sign the ESSA MISA.[13] Non-federal entities, including the private sector, state, local, tribal, and territorial partners, and foreign participants may join AIS after agreeing to a *Terms-of-Use* that outline what information can be submitted and in what form, how that information will be used, who will have access to that information, and how the information is protected. Existing members of DHS's Cyber Information Sharing and Collaboration Program[14] (CISCP), and other similar Government programs, are able to join the AIS initiative by agreeing to the *Terms-of-Use*.

Submission of Indicators or Defensive Measures to the NCCIC

All cyber threat indicators and defensive measures must be submitted in accordance with submission guidance.[15] AIS takes advantage of a technical specification for the format and exchange of cyber threat information using the DHS Structured Threat Information eXchange (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), respectively. STIX is a structured language used to represent the full range of cybersecurity threat information that strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible.[16] TAXII is a DHS-led, community-driven (federal and private sector) effort to standardize a platform for the trusted, automated exchange of cybersecurity threat information online.[17] In short, TAXII is the preferred method of exchanging cybersecurity threat information, which should be input using the STIX language. By using standardized fields (STIX) and communication (TAXII), DHS enables organizations to share structured cyber threat information in a secure and automated manner.

Once a federal or non-federal entity has completed participant entry process by signing the *Terms-of-Use* or ESSA MISA, it may submit cyber threat indicators and defensive measures to the NCCIC by one of three methods:

[13] CISA establishes the Department of Commerce, Department of Defense, Department of Energy, Department of Homeland Security, Department of Justice, Department of Treasury, and the Office of the Director of National Intelligence as federal entities requiring participation in information sharing activities authorized by CISA. These federal entities will still be required to sign the ESSA MISA to receive cybersecurity threat information through AIS.

[14] For more information on CISCP, please visit: https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf.

[15] Submission guidance is provided to participating entities upon signing up for AIS.

[16] For more information on STIX, please visit http://stix.mitre.org/.

[17] TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries for the detection, prevention, and mitigation of cyber threats. TAXII is not an information sharing initiative, and it does not define agreements, governance, or non-technical aspects of cyber threat information sharing. For more information on TAXII, please visit https://taxii.mitre.org/index.html.

- Via the DHS TAXII server in the STIX format using the AIS Profile[18] (for non-federal entities) or ESSA Profile[19] (for federal entities);
- A fillable web form on the US-CERT web portal[20]; or
- Email.

Sharing cybersecurity threat information with DHS through the DHS TAXII server represents the capability and process for sharing cyber threat indicators in real time under CISA. Submissions by web form and email under CISA, if valid, ultimately are re-distributed through the DHS TAXII server, but are not considered a submission under the real time requirement of CISA.

Participants[21] are required to follow submission guidance that outlines the type of information that should and should not be provided when submitting cyber threat indicators or defensive measures through AIS. Specifically, the guidance instructs AIS participants that the indicators and defensive measures[22] they submit should not include PII unless it is directly related to the cybersecurity threat. Participants that submit indicators or defensive measures under the auspices of ESSA are subject to internal guidelines specific to their department or agency that meet the same goal of the submission guidance for non-ESSA entities. DHS uses the AIS Profile to standardize the indicator and defensive measure information and implement a series of automated and manual processes to ensure that unrelated information is removed from the cyber threat indicator or defensive measure before it is disseminated to the AIS participants. Using the AIS Profile in this manner further minimizes privacy, civil liberties, and other compliance risks that may arise when PII and other sensitive information is submitted.

The AIS Profile limits the amount of information in a cyber threat indicator or defensive measure to the information that is directly related to the cybersecurity threat. The AIS Profile is

[18] The AIS Profile is intended to ensure that submissions include input fields most directly related to cyber threat indicators and defensive measures, as assessed by DHS in consultation with other Federal entities. This assessment included a review of STIX fields for privacy, civil liberties, and other compliance concerns and risks. The STIX format includes several thousand fields, whereas the AIS Profile is a subset of those fields that are determined to directly relate to a cybersecurity threat and that otherwise protects privacy and civil liberties as required by CISA. Different indicator types may require the submission of a specific subsection of the fields in the AIS Profile. To see the AIS Profile, please visit: https://www.us-cert.gov/ais.

[19] The ESSA Profile is STIX profile used by the ESSA Community to describe cyber threats to other federal agencies. The ESSA Profile is very similar to the AIS Profile, and when shared with non-federal entities will be translated to the AIS Profile for consistency and to limit confusion amongst participants.

[20] https://www.us-cert.gov/forms/share-indicators

[21] This PIA refers to federal and non-federal entities sharing and receiving cyber threat indicators and defensive measures through AIS collectively as “participants”.

[22] CISA does not require a privacy scrub of defensive measures, however DHS has implemented measures to do so as a matter of policy. In general, defensive measures will not include PII—however the possibility for inclusion does exist, such as including a cyber threat indicator in a defensive measure as a means to describe the type of cyber threat one should take action against. Because of this possible inclusion, DHS has implemented this policy.

constructed to meet the specific scope of the definition of cyber threat indicators and defensive measures in CISA. By narrowly scoping the AIS Profile to those definitions, the expected content of AIS submissions is predictable, thus more easily enabling the usage of automated privacy enhancing controls.

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 specificity and nature of the observable facts are designed to reduce the risk that a cyber threat indicator contains personal content or information inappropriate to share.

In addition to following the submission guidance, a set of minimum requirements must be met, including submitting a minimum number of required data fields (i.e., any field that must be in the AIS Profile in order for the submission to be accepted) to establish the cyber threat indicator or defensive measure. DHS will also automatically reject and delete any prohibited data fields (i.e., any field that is not part of the AIS Profile) that are provided by the submitter.

Pre-Dissemination Processes: PII Review and Removal

Once received, the NCCIC will analyze and process the indicators to validate fields against the AIS profile and remove unrelated PII[23] and other sensitive information prior to dissemination. If an entity submits a cyber threat indicator or defensive measure with data fields beyond what the AIS Profile includes, AIS will automatically delete those prohibited fields and will retain only fields that are part of the profile. AIS then performs a series of automated analyses and technical mitigations to ensure that the information within the data fields meets certain predetermined criteria and does not contain unrelated PII or other sensitive information. These technical mitigations include, but are not limited to: schema restrictions, controlled vocabulary, regular expressions (i.e., pattern matching),[24] known good values,[25] and auto-generated text.

Given that not every AIS submission contains every indicator field and that only a very small percentage of fields trigger a human review, the majority of AIS submissions will be automatically processed and disseminated to AIS participants. However, for those fields for

[23] There are instances where PII may be retained because it is directly related to the cybersecurity threat. For example, information about the cyber threat actor would be retained, but potential victim information would be removed and deleted.

[24] *Schema restrictions, controlled vocabulary,* and *regular expressions* (or, *"pattern matching"*) are methods employed to control the language--in both formatting and vocabulary--used to describe a piece of information. For AIS, these methods ensure that information in a specific data-field contains expected information that can be reviewed by a machine and not contain unrelated PII.

[25] *Known good values* refers to the concept that a piece of information has been previously reviewed and determined not to contain PII or to contain PII that is directly related to the cyber threat. Because of this previous review, that value is now known to be good.

which there is no automated process to determine whether a field contains unrelated PII or other sensitive information, a human analyst at the NCCIC reviews the submission. For example, in certain instances AIS may replace the content of a field with auto-generated text and then place the original potential PII from the indicator in a human-review queue. Some AIS fields may contain information that is not recognizable the first time it is submitted, but upon review by a human analyst becomes a known good value. This known good value is added to the controlled vocabulary of the field and is used to automate the review of the field to the maximum extent possible.

Upon human review, the NCCIC analyst will either:

- Recognize that there is no PII in the field and disseminate the information;
- Determine there is PII in the field directly related to the cybersecurity threat and therefore disseminate the information;
- Determine there is a mix of PII in the field not directly related to the cybersecurity threat and PII and/or non-PII that is directly related to the cybersecurity threat, and therefore manually delete the PII that is not directly related to the cybersecurity threat and disseminate the rest of the information; or
- Determine that the only PII in the field is not directly related to the cybersecurity threat and delete the information from the submission.

While the flagged field is undergoing the human review process, the cyber threat indicator or defensive measure will be disseminated with the field(s) requiring human review replaced with auto-generated text, replacement text, or text indicating removal. Cyber threat indicators and defensive measures that have successfully undergone this pre-dissemination process are considered to be "sanitized." Once human review of the relevant fields is complete, an updated indicator or defensive measure is re-disseminated to the appropriate AIS participants using the versioning feature within STIX.

Dissemination of Cyber Threat Indicators and Defensive Measures

In order to receive cyber threat indicators and defensive measures, AIS participants need to standup or acquire their own TAXII client that will communicate with the DHS TAXII server. The TAXII client has the ability to send machine-to-machine messages in STIX format in an automated fashion, with little-to-no human intervention. This ensures cyber threat indicators and defensive measures are received, analyzed, processed, and disseminated by the NCICC in real-time. AIS participants that are not able to stand up or acquire their own TAXII client may instead rely on the services of organizations (e.g., ISACs or ISAOs) that will share and receive the cyber threat indicators and defensive measures on their behalf.

Once the cyber threat indicator or defensive measure is received, analyzed, and sanitized, AIS will share the indicator or defensive measure with all AIS participants. AIS participants must decide whether they want their identity shared with all AIS participants, only U.S. Government participants, or not with any party at all, when submitting an indicator or defensive measure. If the AIS participant does not populate the consent field in the AIS Profile, AIS will reject its submission. Once a Government department or agency receives a cyber threat indicator through AIS, it can request additional information outside of AIS through other appropriately authorized avenues (e.g., by contacting the information source directly). If the submitting AIS participant's identity is withheld, the government department or agency may request the identity of the indicator submitter from DHS. DHS will only reveal the identity of the indicator submitter as long as the AIS participant has provided consent to do so.

Oversight and Compliance

Over time, the AIS Profile may need to change based on evolving threats or a better understanding of what is needed to analyze cyber threat indicators or explain defensive measures. Any changes to the AIS profile will undergo a privacy, civil liberties, and compliance review that will prescribe technical and manual measures that mitigate privacy risks. This activity is accomplished through an interagency change control board convened by the appropriate federal entities as designated by CISA. Through continued collaboration and experience, the appropriate federal entities and other information sharing participants will identify fields to be added or removed from the AIS Profile. In addition, privacy mitigations will be identified for any such additions. Any change to the AIS Profile will be reviewed by this board and implemented contingent to unanimous consent of the change control board. Further, these changes will be publicly communicated to both the AIS participants and the general public via updates to this PIA, email communications to participants, and in general on the US-CERT.gov website.

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 AIS initiative implements the automated sharing capability as described in the Cybersecurity Information Sharing Act of 2015 (CISA). The AIS capability is not an independent information system, but rather the continuation of an information sharing architecture authorized under the National Cybersecurity Protection System (NCPS).[26] The goal of AIS is to automate this process through privacy-preserving technical approaches and

[26] DHS/NPPD/PIA-026 National Cybersecurity Protection System (NCPS), July 30, 2012, *available at* http://www.dhs.gov/sites/default/files/publications/privacy/privacy-pia-nppd-ncps.pdf.

leveraging the CS&C NCPS infrastructure.

The following authorities permit and define the automated sharing capability required by CISA, NCPS, and related activities:

1) *Cybersecurity Information Sharing Act of 2015* authorizes the sharing of cyber threat information between federal and non-federal entities, requires the development of various guidelines for privacy, civil liberty, and sharing, and provides various protections to non-federal entities for that sharing of that information.

2) *National Cybersecurity Protection Act of 2014*[27] authorizes the National Cybersecurity and Communications Integration Center, including its role as a federal civilian interface for sharing information related to cybersecurity risks and incidents.

3) *Presidential Policy Directive (PPD) 21*[28] advances a national unity of effort 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 entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof.

4) *Federal Information Security Modernization Act*[29] establishes the authorities of the Office of Management and Budget, DHS, and all federal Executive Branch civilian agencies in securing federal information systems. Also establishes a federal information incident security center within DHS. That center is the United States-Computer Emergency Readiness Team (US-CERT).

5) *Homeland Security Act of 2002*[30] provides requirements for alert, warning, and analysis of cyber risks and vulnerabilities to state and local government entities, crisis management support, and technical assistance to private sector and other Government entities. In addition, the Act requires a comprehensive assessment of the vulnerabilities of Critical Infrastructure and Key Resources of the United States and recommended measures necessary of protection.

6) *NSPD-54/HSPD 23*[31] recognizes the need for an organized and unified response to future cyber incidents and to strengthen public-private partnerships to find technology

[27] 6 U.S.C. §§ 148, 149.
[28] *"Critical Infrastructure Security and Resilience,"* February 12, 2013.
[29] 44 U.S.C. § 3551 et seq.
[30] 6 U.S.C §§ 121 and 143.
[31] *Comprehensive National Cybersecurity Security Initiative*, January 8, 2008.

solutions to ensure U.S. security and prosperity.

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

PII collected for registration and consent purposes from AIS Participants to establish the TAXII connection, from email submissions, and from the collection of source information is covered by the DHS system of records titled, DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[32]

PII collected for contact purposes from web form submissions is covered by the DHS system of records titled, DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System.[33]

The content of a cyber threat indicator does not constitute a System of Records under the Privacy Act because information contained within the cyber threat indicators and defensive measures is not retrieved by personal identifier.

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

Yes. The core components of NCPS, which includes the AIS initiative, received their current security authorization in July 2013. The DHS TAXII server was granted a three-year authority-to-operate on January 19, 2016.

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

Yes. The NCPS records retention schedule (Records Schedule Number: DAA-0563-2013-0008), which includes schedules for the disposition of all NCPS data, covers indicators collected as part of the AIS initiative. Section 1.1 of DAA-0563-2013-0008-0001 schedules the disposition of Core Infrastructure information, which includes registration/source information. A second NCPS records schedule (Records Schedule Number: DAA-0563-2015-0008) covers the disposition of operational NCPS data that is inadvertently collected or captured by any or all NCPS capabilities and that are determined not to be related to known or suspected cyber threats or vulnerabilities.

[32] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, (November 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.

[33] DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (November 25, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28053.htm.

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.

DHS will request an OMB Control number for AIS.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

PII regarding AIS participants:

- Individuals representing their agency/organization who establish a DHS TAXII connection (including: name, job title, company, email, telephone number, PKI certificate, electronic signature);
- Individuals representing their agency/organization who submit cyber threat indicators or defensive measures via web form or email (including: name, job title, company name, email, telephone number);
- Individuals who sign an agreement or *Terms-of-Use* (including: name, job title, company, email, telephone number, PKI certificate, electronic signature); or
- Individuals who consent to sharing source and what will be provided (including: name, job title, company, email, telephone number, work address).

Cyber Threat Indicator and Defensive Measure data that could be collected through the AIS profile, including:

- AIS Organization Information (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, etc.); or
- Information or metadata about observables.

Detailed information about what individual data and metadata elements make up an AIS cyber threat indicator or defensive measure can be found in the AIS Profile.[34] Per the submission guidance, submitters should only provide PII that is directly related to the cybersecurity threat. If a submitter includes PII that DHS determines is not directly related to the cybersecurity threat, DHS will remove the PII from the cyber indicator or defensive measure prior to dissemination.

DHS's NCCIC may use the cyber threat indicators and defensive measures provided by AIS to do detailed analysis of cyber threats and cyber threat campaigns for the creation of analytical products, bulletins, and network defense guidance.

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

PII (i.e., contact information) is collected by DHS through TAXII registration, email and web form submissions, signed *Terms-of-Use*, and directly from individuals participating in the AIS initiative.

Cyber threat indicators and defensive measures are submitted to AIS from federal and non-federal entities. Some AIS participants may decide to use a third party, such as an ISAC or ISAO or a security vendor, to submit cyber threat indicators or defensive measures on their behalf.

Indicators may be generated by security software located on the submitting entity's network, but may be manually created as well. Defensive measures will tend to be free form text and not machine generated. For example, a defensive measure may be submitted in the form of white paper, essay, or blog post—but are not necessarily limited to these mediums.

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

NCCIC analysts use information from a range of sources, including commercial sources and publicly available data to verify information on cybersecurity threats (i.e., anything that could be found through open source Internet searches, newspaper articles), which may include indicators submitted by AIS participants.

DHS uses this data to help resolve issues that are reported to NCCIC and for historical reference of similar information. AIS, and NCCIC analysts supporting AIS do not use commercial sources for the purpose of identifying individuals.

[34] For more information about the AIS Profile or for AIS submission guidance, please visit https://www.us-cert.gov/ais.

2.4 Discuss how accuracy of the data is ensured.

The NCCIC is not able to validate the accuracy of every piece of information within an indicator or defensive measure submitted by an organization due to the sheer volume, anticipated workload, and timing necessary to ensure cyber threat indicators and defensive measures are shared in a real-time manner. AIS participants are required to adhere to submission guidance to ensure proper quality control of information submitted to AIS—in addition to adhering to privacy and other compliance requirements. Per the AIS *Terms-of-Use*, DHS reserves the right to terminate access to AIS for repeated failure to abide by submission guidance.

Finally, through its automated and manual processes, AIS executes a series of automated analyses and technical mitigations that ensure that the indicator information DHS expects to receive is what is actually received. For example, an actual IP address appears in the IP address field instead of a string of text.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: AIS participants may submit STIX fields that are prohibited, or not allowed, in the AIS Profile, which could result in DHS's collection or retention of unrelated information (including unrelated PII). This presents the risk of sharing information (such as victim information or non-threat related information) not directly related to the cybersecurity threat.

Mitigation: AIS deletes any prohibited fields that are submitted, thus preventing prohibited information from being stored or shared. Further, during the creation of the AIS Profile, DHS performed a field-by-field analysis to identify any privacy, civil liberties, or other compliance concerns in each individual field of the AIS Profile. An automated or manual process was, in turn, developed and built into the AIS process to remove unrelated PII and mitigate the associated privacy risk.

Automated processes include a series of regular expressions and comparison to controlled vocabulary to ensure that the information within the data fields are as they are expected and do not contain PII (or any other sensitive information) that is not directly related to the cybersecurity threat. For any review that cannot be performed in an automated fashion, the indicator or defensive measure is subject to human review by an NCCIC analyst.

Privacy Risk: Although DHS has built in extensive automated and manual review processes to remove unrelated PII, there remains a residual privacy risk that these processes may not always identify and remove unrelated PII, thereby disseminating more PII than is directly related to the cybersecurity threat.

Mitigation: DHS will periodically review disseminated cyber threat indicators and defensive measures, and the automated and manual review processes, generally, to assess their effectiveness at reducing privacy risk, specifically in removing PII that is not directly related to the cybersecurity threat and make adjustments, as appropriate. If through these periodic reviews DHS determines PII that is not directly related to the cybersecurity threat has been disseminated, DHS will issue an update to the applicable indicator through the versioning feature in STIX. The AIS *Terms-of-Use* contemplate such a scenario and require AIS Participants to use reasonable efforts to promptly apply any necessary versioning updates. In addition, DHS will continue to explore enhancements to the STIX schema, commercial-of-the-shelf products, and other technical solutions that may provide better filtering and dissemination options than what was available at the time of initial development.

Lastly, Section 103(b)(1)(F) of CISA requires procedures for a federal entity to notify, in a timely manner, any United States person whose personal information is known or determined to have been shared in violation of CISA.[35] It should be noted that most personal information exchanged as part of a cyber threat indicator or defensive measure may be incomplete, may not identify a specific individual, or may lack enough information to verify that it pertains to a United States person. However, as a matter of policy, DHS extends individual notification to United States and non-United States persons alike in accordance with its Privacy Incident Handling Guidelines.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

DHS uses PII from AIS participants to certify their agreement to a *Terms-of-Use*, register or connect to TAXII, identify the submitter of web form or email submissions, and for consent (for the onward distribution of source-identity information).

DHS uses information submitted via the AIS Profile to disseminate computer-readable cyber threat indicators and defensive measures to federal and non-federal entities to supplement the existing mostly manual process.

AIS participants use disseminated cyber threat indicators and defensive measures for the uses authorized under CISA. Such authorized uses include:[36]

[35] For DHS's implementation of this provision, DHS will follow their internal Privacy Incident Handling Guidelines (PIHG). For more information on DHS's PIHG, please visit: https://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.

[36] Section 105(d)(5).

1. a cybersecurity purpose;[37]
2. the purpose of identifying (i) a cybersecurity threat, including the source of such cybersecurity threat or (ii) a security vulnerability;
3. the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;
4. the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating a serious threat to a minor, including sexual exploitation and threats to physical safety; or
5. the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in #3 above or any of the offenses listed in (i) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft), (ii) chapter 37 of such title (relating to espionage and censorship), and (iii) chapter 90 of such title (relating to protection of trade secrets).

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.

AIS participants' use of AIS may include queries of indicator information necessary to identify trends and patterns in cyber threat indicators and disparate data sets. Findings from these searches may result in actions taken as authorized under CISA.

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

Only NCCIC analysts and NCPS system administrators have access to the components of the NCPS system used for analysis and reporting of AIS submissions stored within NCPS. This includes federal employees, detailees, and contractor staff that may be assigned analyst or NCPS system administration responsibilities. NCCIC analysts and NCPS system administrators are required by DHS to take basic privacy and security training, as well as training for information handling guidelines specific to CS&C employees.

[37] A Cybersecurity Purpose means protecting an information system (of an AIS Participant, a customer or member of an AIS Participant, or otherwise) or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. Cybersecurity Purpose includes research that is conducted for a Cybersecurity Purpose.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Users of AIS may use AIS cyber threat indicators and defensive measures for purposes other than the uses authorized under CISA.

Mitigation: Government users of AIS cyber threat indicators and defensive measures are required to follow ESSA MISA guidelines that limit their use of cyber threat information and adhere to the Privacy and Civil Liberties Guidelines as required under CISA. Further, non-federal entity users of AIS cyber threat indictors are required to abide by the *Terms-of-Use* of AIS. DHS further mitigates this risk by removing PII that is not necessary to understanding the cyber threat from the cyber threat indicators and defensive measures.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

As with the information sharing authorized under CISA, AIS participation is voluntary. When individuals representing non-federal entities complete the AIS on-boarding process, they are provided notice of the AIS program and why DHS is collecting their information in their respective *Terms-of-Use*. When an AIS participant submits a cyber threat indicator or defensive measure via TAXII, email, or web form DHS will collect basic contact information from him or her.

DHS provides notice for contact information collected via email in an automated response back to the submitter. If an individual submits a cyber threat indicator and/or defensive measure via a web form, his or her contact information is not required, but may be collected. Notice for web form submissions is provided on the web form.

In addition, this PIA and the NCPS PIA serve as a general notice of the AIS initiative.

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

AIS participants agree to a basic level of unattributed sharing of cyber threat indicators and defensive measures upon signing the AIS *Terms-of-Use*. Should an AIS participant consent to sharing his or her identity during the submission process, his or her identity may be disclosed in an automated or manual manner. AIS participants must choose how their identities will be shared; otherwise AIS will reject their submission. Individuals whose PII is included in the cyber threat indicator or defensive measure and is directly related to the cybersecurity threat do not have the opportunity to decline to provide information or opt out of the project.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that DHS will not provide notice to individuals whose personal information is directly related to the cybersecurity threat submitted to DHS.

Mitigation: It is not possible to fully mitigate this risk. DHS has implemented a series of automated and manual procedures to remove PII not directly related to the cybersecurity threat from cyber threat indicators and defensive measures before they are disseminated to the AIS participants. Further, CISA—and by virtue, AIS submission guidance—dictates that AIS participants must remove PII that is not directly related to the cybersecurity threat before they submit cyber threat indicators or defensive measures to AIS.

In addition, this PIA helps provide notice to the public that their PII may be submitted via AIS. This PIA further explains processes put into place to ensure unrelated PII does not get disseminated.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

Indicators, defensive measures, and the identity of the indicator submitter will be retained by DHS, except PII not directly related to the cybersecurity threat, which will be deleted upon automated or manual identification and will not be retained. Indicators and defensive measures that have successfully undergone the pre-dissemination process are considered to be “sanitized.”

Indicators and defensive measures that potentially contain PII not directly related to the cybersecurity threat may be temporarily retained in a human review queue if the automated review process refers it for human review. These indicators and defensive measures are not retrievable by AIS participants and any PII not directly related to the cybersecurity threat that is discovered upon human review will be deleted and will not be retained.

The NCPS records retention schedule, which includes schedules for the disposition of all NCPS data, to include cyber threat indicators and defensive measures collected as part of the AIS initiative was approved by NARA on January 12, 2015 (Records Schedule Number: DAA-0563-2013-0008). A second NCPS records schedule (Records Schedule Number: DAA-0563-2015-0008) covers the disposition of operational NCPS data that is inadvertently collected or captured by any or all NCPS capabilities and that are determined not to be related to known or suspected cyber threats or vulnerabilities.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Due to potential large volumes and resource constraints, a cyber threat indicator or defensive measure may remain in a human review queue longer than it is intended to be retained. This may result in unrelated PII being retained for an indeterminate amount of time.

Mitigation: The volume of cyber threat indicators and defensive measures that will be submitted by private companies though the AIS initiative is unknown and DHS is without precedent to predict the volume. As a result, the best application of resources (such as NCCIC analysts) can only be applied with time and experience. As DHS gains a better understanding of the volume of submissions, resources will be applied to human review processes as appropriate. This will address any potential backlog and timing concerns.

Metrics will be developed to aid in the distribution of resources and in determining the impact of manual review. In addition, NCCIC analysts are required to review all data collected to determine whether information that could be considered PII exists and whether it is directly related to the cybersecurity threat. CS&C guidelines and standard operating procedures (SOP) provide the procedures for marking and handling of PII collected as well as handling and dissemination instructions. The timing associated with executing these guidelines will further aid in determining the amount of resources that need to be applied to the human review queue.

Privacy Risk: PII directly related to the cybersecurity threat could no longer become necessary over time.

Mitigation: In addition to developing a retention schedule for the DHS retention of cyber threat indicators and defensive measures, AIS submissions include supplementary fields for understanding an indicator’s “time to live” or times or frequency cited. Fields such as “time to live” or times or frequency cited indicate the duration in which a cyber threat could be seen in the “wild,” or has been seen in the wild. These fields help individuals analyzing these indicators better decide if an indicator is still indicative of a cyber threat, thus ensuring the PII is still directly related to the cyber threat.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

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.

Source information may be shared via consent of the AIS participant. The NCCIC will process cyber threat indicators and defensive measures and disseminate them to all AIS participants, which includes federal and non-federal entities, for cybersecurity purposes and uses as authorized under CISA. In order to receive AIS cyber threat indicators and defensive measures, federal agencies must be a signatory to the ESSA MISA and non-federal entities must sign the *Terms-of-Use*.

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

AIS shares point-of-contact information about AIS participants with other AIS participants, provided there is consent from the submitter.

Information contained within cyber threat indicators and defensive measures as a part of AIS does not constitute a System of Records under the Privacy Act because cyber threat indicator information is not retrieved by personal identifier.

6.3 Does the project place limitations on re-dissemination?

ISACs and ISAOs may re-disseminate cyber threat indicators and defensive measures to their member organizations. Sector Specific Agencies may re-disseminate derivative products based on AIS indicators and defensive measures to the organizations they are responsible for overseeing. Further dissemination of indicators and defensive measures is controlled via instructions in the AIS submission guidance to AIS participants on how indicators and defensive measures should be treated or disseminated by a receiving organization.

Cyber threat information received through AIS is reviewed to determine if it contains PII and if so, that information is reviewed and only disseminated if sharing the actual information is directly related to the cybersecurity threat.

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

Information contained within cyber threat indicators and defensive measures as a part of

AIS does not constitute a System of Records under the Privacy Act; nonetheless, DHS does maintain an accounting of AIS participants and the indicators and defensive measures it has disseminated.

Some analytical products may be derived from cyber threat indicators and defensive measures submitted through the AIS initiative. As noted in the NCPS PIA, CS&C provides cyber-related information to the public, federal departments and agencies, state, local, tribal, and international entities through a variety of products, many of which are available on the US-CERT.gov website as well as other information sharing tools and portals.

No formal reports disseminated to the US-CERT public website contain PII. Each report is numbered and catalogued and references exist in all products to tie back to a single event or series of events that precipitated the product itself.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that unrelated information, such as victim information or PII not directly related to a cyber threat, may be shared with members of the law enforcement or intelligence community for purposes unrelated to an authorized use under CISA.

Mitigation: DHS's receipt and dissemination of information for the AIS initiative is designed to adhere to purpose specification practices, data minimization practices, sanitization methods, and retention policies. This ensures that AIS and its participants do not receive or share more information than is directly related to a cyber threat.

Purpose Specification. In the *Terms-of-Use*, DHS describes the purpose of AIS to be the exchange of timely, relevant, and actionable cyber threat indicators and defensive measures amongst and between AIS Participants and the Federal Government for a "Cybersecurity Purpose." A Cybersecurity Purpose means protecting an information system (of an AIS Participant, a customer or member of an AIS Participant, or otherwise) or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. Cybersecurity Purpose includes research that is conducted for a Cybersecurity Purpose.

Data Minimization. DHS makes clear in the AIS *Terms-of-Use* and AIS Submission Guidance the type of information that is expected to be submitted for the AIS initiative. AIS participants are to only submit *cyber threat indicators and defensive measures* and may not submit other information such as cyber incidents, customer information, et al. DHS further clarifies the expected information through the AIS Profile. The AIS Profile limits the amount of information participants can submit to DHS by providing a limited set of data fields, various controlled vocabularies, expected schemas, and other technical mitigations. DHS determined that the limited data elements in the AIS Profile are directly related to cyber threats.

Sanitization. Although DHS makes clear what it expects to receive in an AIS submission, it is understood that entities may accidentally submit unrelated or prohibited information. Information that does not belong in the AIS Profile is automatically discarded without any human review. For allowable data elements, DHS employs various sanitization techniques to remove PII not directly related to the cybersecurity threat and prevent further dissemination through AIS. These techniques include the usage of regular expressions to ensure the content of data elements conform to a pattern, controlled vocabulary, expected schema, and other technical mitigations. If an automated technique is not available or able to remove PII within a data element that is not directly related to the cybersecurity threat, then that data element is placed in a queue for human review and not shared until appropriately resolved.

Retention. PII not directly related to the cybersecurity threat is deleted upon automated or manual identification and is not retained. PII may be temporarily retained in a human review queue, but DHS plans to actively monitor the queue and apply resources as appropriate to ensure the information is not retained in the queue longer than intended.

Privacy Risk: AIS submissions may be inappropriately re-disseminated outside of AIS.

Mitigation: This risk is partially mitigated. DHS requires AIS participants to abide by either the ESSA MISA or sign the AIS *Terms-of-Use* that defines allowable dissemination (such as for what indicators may be used, and with whom they may be shared) consistent with those authorized uses under CISA. AIS participants must abide by these agreements. Frequent failure to abide by these agreements may result in the termination of the organization's participation in the AIS initiative.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

For PII collected for the purposes of establishing a TAXII connection, signing the *Terms-of-Use*, manually submitting an indicator via web form/email, or identity information provided for consent, AIS Participants may contact the NCCIC directly at TAXIIADMINS@US-CERT.GOV.

Individuals whose PII has been submitted as part of a cybersecurity threat (and has been deemed directly related to the cyber threat) may not access their information. CISA creates general FOIA exemptions for cyber threat indicators and defensive measures because this information is provided voluntarily by any given entity and is considered the commercial, financial, and proprietary information of such entity. Section 104(d)(4)(B) of CISA exempts cyber threat indicators and defensive measures from disclosure under any provision of state, tribal, or local freedom of information law and similar disclosure laws. Section 105(d)(3) of CISA exempts cyber threat indicators and defensive measures from disclosure under FOIA and withholds this information without discretion, from the public under Section 552(b)(3)(B) of FOIA[38]. Cyber threat indicators and defensive measures are not maintained in a Privacy Act System of Records; therefore individuals are unable to access their information under the Privacy Act. Individuals may still submit a Freedom of Information Act (FOIA) request to the DHS/NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380. Because CISA creates a FOIA exemption, individuals are unable to access their information under the FOIA.

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

Should an individual wish to submit a correction for PII collected for the purposes of establishing a TAXII connection, signing the *Terms-of-Use*, manually submitting an indicator via web form/email, or identity information provided for consent AIS Participants may contact the NCCIC directly at TAXIIADMINS@US-CERT.GOV with the information that they wish to be corrected.

An individual whose PII has been submitted as a part of the cyber threat (and has been deemed directly related to the cybersecurity threat) may not correct his or her information. These individuals are not granted a right to access, correct, or amend these records under the Privacy Act because cyber threat indicators are not maintained in a System of Records.

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

For PII collected for the purposes of establishing a TAXII connection, signing the *Terms-of-Use*, manually submitting an indicator via web form or email, or identity information provided for consent, individuals are notified of the procedures to correct information through this PIA and the DHS/ALL-004[39] and DHS/ALL-002[40] SORNs.

An individual whose PII has been submitted as a part of the cyber threat (and has been deemed directly related to the cybersecurity threat) may not correct his or her information.

[38] 5 U.S.C. § 552(b)(3).

[39] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, (November 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm

[40] DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659, (November 25, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28053.htm

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is risk that an individual whose PII has been submitted as a part of the cyber threat, either inadvertently or legitimately, may not access or correct his or her information.

Mitigation: This risk is partially mitigated in that PII that is not directly related to the cybersecurity threat is deleted through the technical and manual processes described in this PIA. In addition, in the AIS *Terms-of-Use*, each AIS participant agrees that, in the event that it discloses cyber threat indicators or defensive measures by mistake, in error, or without their appropriate Information Handling Level (through mismarking or a failure to mark), it shall promptly notify the NCCIC and take all reasonable steps to mitigate, including sending a versioning update, as soon as it is able.

This risk cannot be fully mitigated in that access and correction to PII that is directly related to the cyber threat would alter the observation reported in the cyber threat indicator or defensive measure and would no longer accurately convey an observation made at that specific point in time. Further, these individuals are not granted a right to access, correct, or amend these records under the Privacy Act because cyber threat indicators and defensive measures are not maintained in a System of Records.

Individuals may still submit a Freedom of Information Act (FOIA) request to the DHS/NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380.Because CISA creates a FOIA exemption, individuals are unable to access their information under the FOIA. Section 104(d)(4)(B) of CISA exempts cyber threat indicators and defensive measures from disclosure under any provision of state, tribal, or local freedom of information law and similar disclosure laws. Section 105(d)(3) of CISA exempts cyber threat indicators and defensive measures from disclosure under FOIA and withholds this information without discretion, from the public under Section 552(b)(3)(B) of FOIA.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

The AIS initiative follows the same procedures as previously identified and published in the NCPS PIA. The AIS Submission Guidance and *Terms-of-Use* provide requirements to ensure information is being appropriately submitted to AIS. DHS also employs technical and manual mitigations and sanitization procedures that provide additional assurance that PII not directly related to the cybersecurity threat is removed from the submission. In addition, DHS will periodically audit and review the submission history of AIS participants and their compliance with AIS *Terms-of-Use*/ESSA MISA and submission guidance. The audit and review will also be to ensure the technical mitigations are working appropriately and that the NCCIC analysts are appropriately sanitizing indicators and defensive measures.

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

Access to the AIS data within NCPS is restricted to individuals with a demonstrated need for access, and such access must be approved by the supervisor as well as the Security Manager. Users must sign Rules of Behavior that identify the need to protect PII prior to gaining access. All NCPS users are trained to protect privacy information. Their actions are logged, and they are aware of that condition. Failure to abide by the Rules of Behavior may result in access being removed, disciplinary measures, and potential termination of employment.

All DHS employees are required to complete annual Privacy Awareness Training. When each DHS employee completes the training, it is recorded in the employee’s file online. In addition, US-CERT analysts and other persons who might come into contact with sensor or other data receive annual training on privacy, legal, and policy issues specifically related to US-CERT operations. This training includes how to address privacy during the development of new signatures, how to generate a report that minimizes the privacy impact, and how to report when a signature seems to be collecting more network traffic than is directly required to analyze the malicious activity.

AIS participants are provided with submission guidance and additional explanatory materials to ensure participants adhere to proper indicator submission procedures.

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

DHS ensures the appropriate distribution of AIS cyber threat indicators and defensive measures through the use of data tagging and access controls specification. These tools ensure that only the appropriate entities receive AIS indicators and defensive measures and source identity information is only shared with those entities when the AIS participant has provided consent.

Federal entities accessing cyber threat indicators and defensive measures through AIS are subject to the ESSA MISA, which federal entities are required to sign to participate in AIS. The ESSA MISA prescribes a series of handling guidelines to which Government entities must adhere in regards to cyber information sharing.

Non-federal entities accessing cyber threat indicators and defensive measures through AIS are subject to the AIS *Terms-of-Use*. These prescribe ground rules that non-federal entities must follow and submission guidance with which these entities must strive to adhere in regards to cyber information sharing.

Procedures governing access for the NCPS are covered in the NCPS PIA.[41]

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?

DHS Privacy and the NPPD Office of Privacy participated in the development of the ESSA MISA and the AIS *Terms-of-Use*. In addition, privacy points of contact covering multiple federal agency equities participated in this review process. This collaboration ensured privacy was incorporated into AIS from the beginning. As AIS is adopted and expands, information contained in the AIS Profile used to describe a cyber threat indicator or defensive measure may change over time. Conversely, changes to the understanding of a cyber threat indicator or defensive measure may change over time, necessitating an update to the AIS Profile. The changes to the AIS Profile will be managed through an interagency change process that will consider all relevant privacy, civil liberties, and compliance concerns.

Responsible Officials

Andy Ozment
Assistant Secretary, Office of Cybersecurity & Communications
National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

[41] DHS/NPPD/PIA-026 National Cybersecurity Protection System (NCPS), July 30, 2012, *available at* http://www.dhs.gov/sites/default/files/publications/privacy/privacy-pia-nppd-ncps.pdf.