Privacy Impact Assessment
for the

Automated Indicator Sharing (AIS)

DHS/NPPD/PIA-029

October 28, 2015

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 among the private sector and government departments and agencies. These cyber threat indicators are shared for the purposes of network defense, cybersecurity, and research purposes and in a manner that ensures appropriate incorporation of privacy, civil liberties, and other compliance protections. Central to the AIS initiative, the DHS National Cybersecurity and Communications Integration Center (NCCIC) serves as the centralized hub for exchanging cyber threat indicators 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.

Overview

The Department of Homeland Security (DHS) National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C), consistent with the National Cybersecurity Protection Act of 2014[1] and Presidential Policy Directive (PPD)-21,[2] has developed the Automated Indicator Sharing (AIS) initiative to enable private companies, nonprofit organizations, academia, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs),[3] and Government departments and agencies to share indicators of cybersecurity threats.

The goal of the AIS initiative is to achieve near real-time sharing of cyber threat[4] indicators by enabling DHS's National Cybersecurity and Communications Integration Center (NCCIC) to (1) receive indicators from the private sector; (2) remove unnecessary personally identifiable information and other sensitive information;[5] and (3) disseminate the indicators to, as appropriate, other Government departments and agencies and the private sector.

---

[1] Pub. L. No. 113-282, https://www.congress.gov/113/bills/s2519/BILLS-113s2519es.pdf.
[2] Presidential Policy Directive (PPD)-21: "Critical Infrastructure Security and Resilience," February 12, 2015, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[3] Information Sharing and Analysis Organizations (ISAOs), and by inclusion Information Sharing and Analysis Centers (ISACs), 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.
[4] For AIS, a "cyber threat" is defined as any action that may result in unauthorized access in order to damage or impair the integrity, confidentiality, or availability of an information system or unauthorized exfiltration, deletion, or manipulation of information that is stored on, processed by, or transiting an information system, except that exceeding authorized access of an information system shall not be considered a cyber threat if such access solely involves a violation of consumer terms of service or consumer licensing agreements.
[5] In addition to PII, sensitive information could include, but is not limited to, Proprietary Information, Export Controlled Information, or other business sensitive information. For certain compliance information, such as Proprietary Information, the submitting entity will have to identify that information (as it is in the best position to do

The successful implementation of AIS will support federal departments, agencies, and the private sector in addressing cyber threats 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

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

- **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.
- **Final Phase:** Fully automate DHS processes to receive and appropriately disseminate cyber threat indicators in a machine-readable format and finalize policies for filtering, receipt, retention, use, and sharing, including regular compliance reviews.
- **Shared Services:** Implement a shared services capability that helps federal departments and agencies participate in automated cyber threat indicator sharing regardless of cybersecurity sophistication or resources.

As each phase is developed, DHS will update this PIA, as appropriate.

AIS Participation

All federal departments and agencies, and private sector entities, state, local, tribal, and territorial partners, as well as foreign governmental and foreign private sector entities are eligible to participate in the AIS initiative. During the initial phase of AIS, however, participants will include only limited federal departments and agencies and select private sector entities. All federal departments and agencies that participate in the initial phase of AIS are existing partners under the Enhance Shared Situational Awareness (ESSA)[6] Multilateral Information Sharing Agreement (MISA), which defines rules, guidelines, and policies for Government sharing of cyber

so). In that case, the submitting entity would use a flag that indicates as such. The compliance review process for all sensitive information is the same – automated review followed by human review if, necessary.

[6] 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.

information. To receive indicators through AIS, participating federal departments and agencies are required to sign the ESSA MISA. Private sector, state, local, tribal, and territorial partners, and foreign participants may join AIS after agreeing to a *Terms-of-Use* that outlines 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[7] (CISCP), and other similar Government programs, are able to join the AIS initiative by agreeing to the *Terms-of-Use*.

Submission of Indicators to the NCCIC

All cyber threat indicators must be submitted in accordance with submission guidance.[8] AIS leverages 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 cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible.[9] TAXII is a DHS-led, community-driven effort to standardize the trusted, automated exchange of cyber threat information.[10] In short, TAXII is the preferred method of exchanging cyber 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 department, agency, or private sector entity has completed participant entry process through signing the *Terms-of-Use*, it may submit cyber threat indicators to the NCCIC by one of three methods:

- Via the DHS TAXII server in the STIX format using the AIS Profile;[11]
- A fillable web form on the US-CERT web portal; and/or
- Email.

[7] For more information on CISCP, please visit: https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf.
[8] For more information of AIS submission guidance, please visit https://www.us-cert.gov/ais.
[9] For more information on STIX, please visit http://stix.mitre.org/.
[10] 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.
[11] The AIS Profile is a selection of the STIX fields that most directly relate to cyber threat indicator sharing and that have been assessed by the interagency AIS Privacy & Compliance Working Group 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 approximately 300 fields that DHS determined are necessary for the initial phases of AIS. Not all 300 fields are expected to be populated in an AIS indicator, as different indicator types may require the submission of a specific subsection of those fields. To see the AIS Profile, please visit: https://www.us-cert.gov/ais.

Participants are required to follow submission guidance that outlines the type of information that should and should not be provided when submitting cyber threat indicators through AIS. Specifically, the guidance instructs AIS participants that the indicators they submit should not include PII unless it is necessary to understanding the cyber threat. Participants that submit indicators 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 information and implement a series of automated and manual processes to ensure unnecessary information is removed from the cyber threat indicator 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, in addition to the submission guidance and ESSA requirements that discourage the submission of unnecessary information.

The AIS Profile limits the amount of information in a cyber threat indicator to the information that is needed to understand the cyber threat. Much of the information within an indicator is centered on an observable—a fact about the cyber threat. For example, "observables"[12] in a cyber threat indicator may include: malicious email, internet protocol (IP) addresses, file hashes, domain names, uniform resource locators (URLs), and malware artifacts (attributes about a file). Metadata about these observables are also found in the indicator. For example, metadata about a malicious email may include the From Address/Sender, Subject Line, Message ID, and X-Mailer (or, "email client"). The specificity of the observables, and the metadata about the observables, ensure a cyber threat indicator does not result in the over collection of information.

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 indicator. 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 unnecessary PII[13] and other sensitive information prior to dissemination. If an entity submits a cyber threat indicator with data fields beyond what the AIS Profile includes, those prohibited fields will be automatically deleted and only fields that are part of the profile are retained. AIS then performs a series of automated analyses and technical mitigations to ensure that the information within the data fields meets certain predetermined

[12] Observed facts about a cyber threat, *e.g.*, email messages, IP Addresses, URIs, Hashes, or Files.
[13] While this information may normally be considered personally identifiable information, the information retained is necessary to understanding the cyber threat. Information not necessary will be removed and deleted. For example, information about the cyber threat actor would be retained, but potential victim information would be removed and deleted.

criteria and does not contain unnecessary PII or other sensitive information. These technical mitigations include, but are not limited to: schema restrictions, controlled vocabulary, regular expressions (i.e., pattern matching),[14] known good values,[15] and auto-generated text.

Given that not every AIS submission contains every indicator field and that only a very small percentage of indicator fields trigger a human review, the majority of AIS submissions will be automatically processed and disseminated to AIS participants. However, for those fields for which there is no automated process to determine whether an indicator field contains unnecessary PII or other sensitive information, a human analyst at the NCCIC reviews the indicator. For example, in certain instances AIS replaces the content of a field with auto-generated text and then places 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 necessary to understanding the cyber threat, and therefore disseminate the information;
- Determine there is only PII in the field that is not necessary to understanding the cyber threat so the information is removed from the Record and not disseminated. If the information relates to threats or acts of terrorism, abuse of minors including sexual exploitation, and threats to physical safety, serious bodily harm, loss of life, or an attempt or conspiracy to commit any of the offenses just described, the information is forwarded to law enforcement entities. Otherwise, the information is deleted.
- Determine there is a mix of PII in the field not necessary to understanding the cyber threat and non-PII that is relevant to the cyber threat, and therefore manually deletes the PII (unless required to be forwarded to law enforcement entities as described above) and disseminate the rest of the information.

While the indicator field is undergoing the human review process, the cyber threat indicator will be disseminated with the indicator field(s) requiring human review replaced with auto-

[14] *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 unnecessary PII.

[15] *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 necessary to understanding the cyber threat. Because of this previous review, that value is now known to be good.

generated text or removed. Indicators that have successfully undergone this pre-dissemination process are considered to be "sanitized." Once human review of the relevant indicator fields is complete, an updated indicator is re-disseminated to the appropriate AIS participants using the versioning feature within STIX.

Dissemination of Cyber Threat Indicators

In order to receive cyber threat indicators, 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 are received, analyzed, processed, and disseminated by the NCICC in near 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 on their behalf.

Once the cyber threat indicator is received, analyzed, and sanitized, AIS will share the indicator with all AIS participants. AIS will not provide the identity of the submitting entity to the other AIS participants unless the submitter consents, initially or upon request by AIS, to share its identity as the source of the cyber threat indicator 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 or as otherwise required by law. The consent process does not supersede legally required disclosures of submitter identity or any other PII so received through AIS to a law enforcement agency (e.g., terrorism investigations, child abuse/pornography investigations, threats to physical safety, of bodily harm, or loss of life). Indicator information pending human review is also subject to these legally required disclosures.

Oversight and Compliance

Over time, the AIS Profile may need to change based on evolving threats or better understanding of what is needed to analyze cyber threat indicators. 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. Further, those changes will be publicly communicated to both the AIS participants and general public via updates to this PIA.

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 is not an independent information-sharing program, but rather the continuation of information sharing activities under the National Cybersecurity Protection System (NCPS).[16] The goal of AIS is to automate this process through privacy-preserving technical approaches and leveraging the CS&C NCPS infrastructure.

The following authorities permit and define the NCPS and its related activities:

1) *National Cybersecurity Protection Act of 2014*[17] 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.

2) *Presidential Policy Directive (PPD) 21*[18] 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.

3) *Federal Information Security Management Act*[19] 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).

4) *Homeland Security Act of 2002*[20] 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.

---

[16] 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.
[17] 6 U.S.C. §§ 148, 149.
[18] **"***Critical Infrastructure Security and Resilience,"* February 12, 2013.
[19] 44 U.S.C § 3546.
[20] 6 U.S.C §§ 121 and 143.

5) *NSPD-54/HSPD 23*[21] recognizes the need for an organized and unified response to future cyber incidents and strengthen public-private partnerships to find technology 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).[22]

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.[23]

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 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 the NCPS, which includes the AIS initiative, received their current security authorization in July 2013. The DHS TAXII server was granted a one-year authority-to-operate on April 10, 2015.

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.

---

[21] *Comprehensive National Cybersecurity Security Initiative*, January 8, 2008.
[22] 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
[23] 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 is working towards receiving 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 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 data:

- Information that could be collected through the AIS profile, including:
  - AIS Organization Information (Name, Sector, Location);
  - Descriptions about the indicator;
  - Observed facts about a cyber threat, or “Observables” (Email messages, IP Addresses, URIs, Hashes, Files, etc.); or
  - Information or metadata about observables.

Detailed information about what individual data and metadata elements make up an AIS indicator can be found in the AIS Profile.[24] Per the submission guidance, submitters should only provide PII that is necessary to understanding the cyber threat. If a submitter includes PII that DHS determines is unnecessary to understanding the cyber threat, DHS will remove the PII from the Indicator prior to dissemination.

DHS's NCCIC may use the cyber threat indicators 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 are submitted to AIS from Government departments and agencies and the private sector. Some AIS participants may decide to use a third party, such as an ISAC/ISAO or a security vendor, to submit cyber threat indicators on their behalf.

Indicators may be generated by security software located on the submitting entity's network, but may be manually created as well.

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. This will allow the NCCIC analysts to identify indicators that present no value (such as an IP Address indicator that points to a non-malicious computer) and factor into decision whether to distribute further information on the indicator to the AIS community. DHS anticipates automating this process.

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.

[24] 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 submitted by an organization due to the sheer volume, anticipated workload, and timing necessary to ensure cyber threat indicators are shared in a near-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. 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 unnecessary information (including unnecessary PII). This presents the risk of sharing information (such as victim information or non-threat related information) not relevant to the understanding of the cyber 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 unnecessary 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 necessary to understanding the cyber threat. For any review that cannot be performed in an automated fashion, the indicator is subject to human review by an NCCIC analyst.

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

Mitigation: DHS will periodically review disseminated cyber threat indicators, and the automated and manual review processes, generally, to assess their effectiveness at reducing privacy risk, specifically in removing PII that is not necessary to understanding the cyber threat

and make adjustments, as appropriate. If through these periodic reviews DHS determines PII that is not necessary to understanding the cyber 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.

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/connect to TAXII, identify the submitter of web form/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 to federal departments and agencies and limited private sector partners to supplement the existing mostly manual process.

AIS participants use disseminated cyber threat indicators for the purposes of network defense.

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 for network defense.

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 indicators 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.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Users of AIS may use AIS cyber threat indicators for purposes other than network defense.

Mitigation: Government users of AIS cyber threat indicators are required to follow ESSA MISA guidelines that limit their use of cyber threat information. Further, private sector users of AIS cyber threat indictors are required to abide by the Terms-of-Use of AIS. Lastly, DHS further mitigates this risk by removing PII that is not necessary to understanding the cyber threat from the cyber threat indicators.

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.

AIS participation is voluntary. When individuals or entities complete the AIS on-boarding process via ESSA, 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 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 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 upon signing the AIS *Terms-of-Use*. Should an AIS participant consent, his/her identity may be disclosed in an automated or manual manner. However, by default, the identity of AIS participants will not be revealed to the AIS community. Individuals whose PII is included in the cyber threat

indicator and is necessary to understand the cyber 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 information is necessary to understand the cyber threat indicators 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 necessary to understanding the cyber threat from cyber threat indicators before those indicators are disseminated to the AIS participants. Further, submission guidance dictates that AIS participants must remove PII that is not necessary to understanding the cyber threat before they submit cyber threat indicators 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 unnecessary 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 and the identity of the indicator submitter will be retained by DHS, except that PII not necessary to understanding the cyber threat will be deleted upon automated or manual identification and will not be retained, except in narrow cases for law enforcement purposes as explained in section 6.5. Indicators that have successfully undergone the pre-dissemination process are considered to be "sanitized."

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

DHS is working with the National Archives and Records Administration to schedule cyber-threat indicators submitted to DHS for the AIS initiative. The NCPS records retention schedule, which includes schedules for the disposition of all NCPS data, to include indicators 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 may remain in a human review queue longer than a cyber threat indicator is intended to be retained. This may result in unnecessary PII being retained for an indeterminate amount of time.

Mitigation: The volume of indicators 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 indicators submitted, 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 germane 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 necessary to understanding the cyber threat could no longer become necessary over time.

Mitigation: In addition to developing a retention schedule for the DHS retention of cyber threat indicators, AIS indicators include supplementary fields for understanding an indicator's "time to live" or times/frequency cited. Fields such as "time to live" or times/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 necessary to understanding 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 both consent of the AIS participant or by legally required disclosure to a law enforcement agency. The NCCIC will process cyber threat indicators and disseminate them to all AIS participants, which includes federal agencies outside of DHS and private sector entities, for network defense purposes. In order to receive AIS cyber threat indicators, federal agencies must be a signatory to the ESSA MISA and private sector 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 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/ISAOs may re-disseminate cyber threat indicators to their member organizations. Sector Specific Agencies may re-disseminate derivative products based on AIS indicators to the organizations they are responsible for overseeing. Further dissemination of indicators is controlled via instructions in the AIS submission guidance to AIS participants on how indicators 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 necessary to understanding the cyber threat. If PII needs to be disseminated (such as certain categories of criminal activity discovered during human review) to external stakeholders, written approval must be obtained from CS&C leadership in advance of dissemination, in accordance with CS&C guidelines and SOPs.

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

Information contained within cyber threat indicators 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 it has disseminated.

Some of these products may be derived from cyber threat indicators 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. In the event that PII must be released, it is released in accordance with the appropriate SOPs and with the authorization and/or written approval of CS&C leadership and in compliance with the Privacy Act.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that unnecessary information, such as victim information or PII not necessary to understanding a cyber threat, may be shared with members of the law enforcement or intelligence community for purposes unrelated to cybersecurity.

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 necessary to understand a cyber threat. However, there are some types of information that DHS is legally obligated to forward on to law enforcement entities even if such information is not relevant to AIS.

Purpose Specification. In the *Terms-of-Use*, DHS describes the purpose of AIS to be the exchange of timely, relevant, and actionable indicators amongst and between AIS Participants and the Federal Government for our collective cybersecurity, the cybersecurity of AIS Participant's members and customers, and cybersecurity-related research efforts.

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 not 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 necessary to understand cyber threat indicators.

Sanitization. While DHS makes clear what it expects to receive in a cyber threat indicator submission, it is understood that entities may accidentally submit unnecessary 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 necessary to understanding the cyber 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 and/or able to remove PII within a data element that is not necessary to understanding the cyber threat, then that data element is placed in a queue for human review and not shared until appropriately resolved.

Retention. PII not necessary to understanding the cyber 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 indicator information is not retained in the queue longer than intended.

Exceptions for Law Enforcement Disclosure related to Specific Threats and Crimes. The *Terms-of-Use* also provides that DHS will disclose to federal law enforcement entities information provided through AIS that relates to threats or acts of terrorism, abuse of minors including sexual exploitation, and threats to physical safety, serious bodily harm, loss of life, or an attempt or conspiracy to commit any of the offenses just described.

Privacy Risk: AIS indicators 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). 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.

An individual whose PII has been submitted as a part of the cyber threat (and has been deemed necessary to understanding the cyber threat) may not access his or her information because cyber threat indicators are not maintained in a System of Records. Individuals may submit Freedom of Information Act (FOIA) requests to the DHS/NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380.

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 necessary to understanding the cyber 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/email, or identity information provided for consent, individuals are notified of the procedures to correct information through this PIA and the DHS/ALL-004[25] and DHS/ALL-002[26] SORNs.

[25] 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
[26] DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659,

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

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 necessary for understanding the cyber threat is deleted through the technical and manual processes described in this PIA. However this risk cannot be fully mitigated in that access and correction to PII that is necessary to understanding the cyber threat would be counter to the utility of the cyber threat indicator. Further, 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.

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 necessary to understanding the cyber 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.

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

(November 25, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28053.htm

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

Federal entities accessing indicators 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.

Private sector entities accessing indicators through AIS are subject to the AIS *Terms-of-Use*. These prescribe ground rules that private sector 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.[27]

[27] 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.

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 for a cyber threat indicator may change over time. Conversely, changes to the understanding of a cyber threat indicator 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