Privacy Impact Assessment

for

EINSTEIN 3 - Accelerated (E^3A)

April 19, 2013

DHS/PIA/NPPD-027

Contact Point
Brendan Goode
Director, Network Security Deployment
Office of Cybersecurity & Communications
National Protection and Programs Directorate
Department of Homeland Security
(703) 235-2853

Reviewing Official
Jonathan Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C) continues to improve its ability to defend federal civilian Executive Branch agency networks from cyber threats. Similar to EINSTEIN 1 and EINSTEIN 2, DHS will deploy EINSTEIN 3 Accelerated (E^3A) to enhance cybersecurity analysis, situational awareness, and security response. With E^3A, DHS will not only be able to detect malicious traffic targeting federal government networks, but also prevent malicious traffic from harming those networks. This will be accomplished through delivering intrusion prevention capabilities as a Managed Security Service provided by Internet Service Providers (ISP). Under the direction of DHS, ISPs will administer intrusion prevention and threat-based decision-making on network traffic entering and leaving participating federal civilian Executive Branch agency networks.

This Privacy Impact Assessment (PIA) is being conducted because E^3A will include analysis of federal network traffic, which may contain personally identifiable information (PII).

Overview

National Cybersecurity Protection System

In 2008, in response to expanding cybersecurity mission requirements from Congress and the Administration, the National Cybersecurity Protection System (NCPS)[1] was established to protect the federal civilian Executive Branch government network and prevent known or suspected cyber threats.[2] Network Security Deployment (NSD), a branch of the Office of Cybersecurity and Communications (CS&C), serves as the NCPS Program Office and leads the development and implementation of the NCPS, which provides cybersecurity technologies to continuously counter emerging cyber threats and apply effective risk mitigation strategies to detect and deter these threats. NSD works with all of the CS&C branches to ensure that NCPS capabilities deployed by NSD support and augment the mission capabilities of those branches.

EINSTEIN 3 Accelerated (E^3A)

The NCPS includes an intrusion prevention capability, operationally known as E^3A. With E^3A, DHS will not only be able to detect malicious traffic targeting federal

[1] The NCPS and EINSTEIN related PIAs can be found at: http://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd.

[2] Cyber threats can be defined as any identified efforts directed toward accessing, exfiltrating, manipulating, or impairing the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority. Information about cyber threats may be received from government, public, or private sources. Categories of cyber threats may include, for example: phishing, IP spoofing, botnets, denials of service, distributed denials of service, man-in-the-middle attacks, or the insertion of other types of malware.

government networks, but also prevent malicious traffic from harming those networks. E^{3}A allows DHS to better detect, respond to, and appropriately counter, known or suspected cyber threats identified within the federal network traffic it monitors. E^{3}A monitors only select Internet traffic either destined to, or originating from, federal civilian Executive Branch departments and agencies (commonly known as the ".gov" traffic).

CS&C delivers E^{3}A intrusion prevention capabilities as a Managed Security Service provided by Internet Service Providers (ISP). Managed Security Services is a model by which the government articulates requirements that address the objectives and service levels expected for their constituencies. Under such a model, Managed Security Service providers determine how those services will be delivered.

E^{3}A provides capabilities beyond those implemented in EINSTEIN 1 and EINSTEIN 2. In brief, EINSTEIN 1 analyzes network flow records and EINSTEIN 2 detects and alerts[3] to known or suspected cyber threats using Intrusion Detection Systems (IDS) technology. EINSTEIN 2's network IDS technology uses custom signatures,[4] based upon known or suspected cyber threats within federal network traffic. E^{3}A supplements EINSTEIN 2 by adding additional intrusion prevention capabilities and enabling ISPs, under the direction of DHS, to detect and block known or suspected cyber threats using indicators.[5] The source of information analyzed by the ISPs will be federal network traffic transiting to or from the participating agencies. This network traffic is defined by the list of IP addresses supplied by each agency and verified by DHS and agency's E^{3}A servicing ISP. Initially, E^{3}A will use two cyber threat countermeasures:[6]

1) The Domain Name Server (DNS) Sinkholing capability allows DHS to prevent malware installed on .gov networks from communicating with known or suspected malicious Internet domains (sinkhole information) by redirecting the network connection away from the malicious domain to "safe servers" or "sinkhole servers," thus preventing further malicious activity by the installed malware. The ISP has access to the sinkhole information. However, the information related to the attempted connection that can be gathered by the

[3] An alert, in the context of the EINSTEIN capabilities, is when the system alerts a human analyst to suspected malicious activity.

[4] Signatures are specific machine readable patterns of network traffic that affect the integrity, confidentiality, or availability of computer networks, systems, and information. For example, a specific signature might identify a known computer virus that is designed to delete files from a computer without authorization. For the purposes of this PIA, signatures and indicators are collectively referred to as "indicators."

[5] An indicator can be defined as human-readable cyber data used to identify some form of malicious cyber activity and are data related to IP addresses, domains, email headers, files, and strings. Indicators can be either unclassified or classified. Classification of identified indicators is dictated by its source.

[6] Countermeasures are tailored to take only those steps necessary to detect, analyze, respond to, or prevent known or suspected cyber threats. Countermeasures will also be tested prior to implementation.

ISP is limited to information related to the DNS request rather than the contents of the intended malicious communication.

2) The Email Filtering capability allows DHS to scan email destined for .gov networks for malicious attachments, Uniform Resource Locators (URL), and other forms of malware, before being delivered to .gov end-users[7]. Depending on the specific implementation by the ISP, infected emails may be quarantined or redirected from the target email address to another location for further inspection for malicious content by CS&C cybersecurity analysts. Only emails deemed malicious – those matching a signature – may be quarantined and further reviewed.

E^{3}A combines existing CS&C analysis of EINSTEIN 1 and EINSTEIN 2 data as well as information provided by cyber mission partners with existing commercial intrusion prevention security services to allow for the near real-time deep packet inspection[8] of federal network traffic to identify and react to known or suspected cyber threats. CS&C will contract with ISPs to provide E^{3}A managed intrusion prevention security services to deploy countermeasures against known indicators in order to better secure the federal networks. Unless otherwise noted, the descriptions and analysis provided in the NCPS PIA and related NPPD PIAs apply to E^{3}A and provide a comprehensive view of the CS&C privacy analysis related to the NCPS program.

Indicators of Known or Suspected Cyber Threats

As part of its mission to promote the protection of cyber infrastructure, CS&C collects information that is specific to identifying known or suspected cyber threats from a number of sources. These "indicators" are used to create intrusion detection signatures for the means of detecting and mitigating cyber threats. Sources for indicators may include individuals with cyber expertise, domestic and international private sector organizations, and international, federal, or state agencies with a vested interest in promoting cybersecurity. Indicators about known or suspected cyber threats may also be collected from information gathered by the EINSTEIN sensors placed on federal agency network collection points.[9]

---

[7] As the capability matures, DHS will likely add additional countermeasures to E^{3}A, but the potential collection and use of PII will remain unchanged. This PIA will be updated to reflect the implementation of any countermeasures not covered in this PIA.

[8] Deep packet inspection means being able to look into the content of cyber traffic to inspect for viruses, spam, or other malicious content. Network flow records contain only packet header information. Packet inspection tools allow an analyst to look at the content of the threat data, which enables a more comprehensive analysis.

[9] These sensors capture flow records that identify the Internet Protocol (IP) address of the computer that connects to the federal system, the port the source uses to communicate, the time the communication occurred, the federal destination IP address, the protocol used to communicate, and the destination port.

An indicator can be defined as human-readable cyber data used to identify some form of malicious cyber activity and are data related to:

1) IP addresses;
2) Domains;
3) E-mail headers;
4) Files; and
5) Strings.

Each characteristic of an indicator contains specific features, for instance:

- IP and Domain Indicators can typically be found in publicly available WHOIS[10] information; Uniform Resource Identifiers[11] (URI) can also obtain IP and domain indicators. URIs are indicators in and of themselves; however, CS&C can also track these indicator types via strings.
- E-mail Indicators can contain message attributes such as the sent date, subject, links, attachments, sender's name, and sender's e-mail address;
- File Indicators can contain information on malware that is designed specifically to damage or disrupt a computer system; and
- String Indicators consist of persistent and unique identifiers specific to malicious activity, such as characters, numbers, or symbols, used to represent a word or phrase.

Indicators can contain varying levels of detail regarding a specific cyber threat and one indicator can have a relationship with another indicator. For example, an e-mail can contain an attachment and that attachment can contain malware.

EINSTEIN indicators and indicator reports are created and validated by CS&C cybersecurity analysts based on indicators of known or suspected cyber threats that are identified and validated by CS&C, private sector organizations, and other partner government agencies. Indicator reports can be produced with any combination of indicators and can have either a single indicator or multiple types of indicators and multiple entries for each type therein. For example, a certain indicator report may contain one email, one file, and one domain; other indicator reports may contain four files, or two domains and three IP addresses. Indicators and indicator reports are shared with ISPs for the purpose of enhancing intrusion prevention capabilities.

[10] WHOIS is a Transmission Control Protocol (TCP)-based transaction-oriented query/response protocol that is widely used to provide information services to Internet users. While originally used to provide "white pages" services and information about registered domain names, current deployments cover a much broader range of information services. The protocol delivers its content in a human-readable format.
[11] URI is the generic term for all types of names and addresses that refer to objects on the World Wide Web. A Uniform Resource Locator (URL) is one kind of URI.

The goal of E^3A, in conjunction with the greater NCPS, is to identify, characterize, and block known or suspected cyber threats in order to enhance cybersecurity analysis, to increase situational awareness, and to enable appropriate security responses in conjunction with, or on behalf of, our federal partners. ISPs participating in E^3A will facilitate the ability to automatically detect and respond appropriately to known or suspected cyber threats before harm is done, thus providing an intrusion prevention security service that reduces cyber risk and assists DHS in protecting federal systems and reducing vulnerabilities on federal civilian Executive Branch networks.

Indicator Sharing Under E^3A

CS&C relies on signatures based on specific indicators that are known or suspected to be associated with malicious activity. While indicators will often be based on network traffic metadata, such as IP addresses, they may potentially be designed to match against any packet data, including the payload (the network traffic data). As such, E^3A prevention capabilities may include deep packet inspection by ISPs. DHS will approve indicators to be transferred to ISPs for deployment in E^3A to ensure that indicators are specific to a particular type of traffic and are not overly broad in their data collection requirements. All indicators developed by CS&C will be reviewed before being transferred to ISPs to ensure that they further the DHS cyber mission. CS&C shares these indicators with ISPs through secure channels. The ISPs then configure the indicators into signatures for testing and implementation and perform pattern matching[12] against established indicators based on known or suspected malicious traffic to or from the participating agencies. ISPs may also submit their own cyber threat indicators to DHS for consideration. These indicators must be reviewed and approved by DHS prior to use.

When an ISP implements signatures on behalf of DHS from information shared through indicators, and that signature triggers an alert, the ISP reports both the fact of occurrence and any additional details regarding the incident to DHS. Alerts and contextual information provided to CS&C by the ISP will generally contain the following information: unique ID for the alert, participating agency, indicator/action pair that produced the alert, date and timestamp of the alert, netflow record, and, if applicable, identification of quarantined or captured/stored data associated with the alert. The nature of the reporting is consistent with data collected and analyzed under the DHS EINSTEIN

[12] Pattern matching is a technique in automated data analysis, usually performed on a computer, by which a group of characteristic properties of an unknown object is compared with comparable groups of characteristics of a set of known objects, to discover the identity or proper classification of the unknown object.

efforts and agency responsibilities under the Federal Information Security Management Act for securing federal agency information systems.

Relationship Between Participants

DHS shares cyber threat information it receives through E^{3}A consistent with its existing policies and procedures, including sharing and coordination with any affected participating federal departments and agencies as well as other federal cybersecurity mission partners.

Participating departments and agencies will enter into a Memorandum of Agreement (MOA) with DHS to authorize the application of intrusion prevention capabilities by DHS. In particular, the MOA establishes the parameters of agency participation in the NCPS program and authorizes the inspection and modification of agency traffic and other interactions with agency information systems in connection with the application of such intrusion prevention capabilities. DHS anticipates that ISPs will also receive a letter of agency or similar agreement from participating departments and agencies notifying ISPs of their agreement to participate in the NCPS program with DHS. The ISPs will provide the services procured via its contract with DHS to only those participating department and agencies that use the contracted ISP(s) as their service provider. The source of information analyzed by the ISPs will be federal network traffic transiting to or from the participating agencies. This network traffic will be defined by the list of IP addresses supplied by each agency and verified by DHS and their E^{3}A-servicing ISP. ISPs are required to follow specific Standard Operating Procedures (SOP) for the implementation of IP addresses, which includes verifying the accuracy of the IP addresses supplied by the agency prior to full implementation and monitoring to identify any traffic that may be outside the range of identified IP addresses. Contracts, service level agreements, and information handling procedures contain provisions to address circumstances where an ISP detects network traffic that is not associated with a participating agency's network.

Privacy Considerations

E^{3}A participating agencies identify a list of IP addresses for their networks and both CS&C cybersecurity analysts and the ISPs verify the accuracy of the list of IP addresses provided by the agency. CS&C and the ISPs perform monitoring to identify any traffic that may be outside the range of identified IP addresses. CS&C SOPs are followed in the event any out-of-range network traffic is identified and the ISP removes any collected data to prevent any further collection of this network traffic.

In addition, CS&C reviews and approves all indicators that are provided to the ISPs to ensure that the corresponding signatures are tailored to only alert and mitigate traffic associated with cybersecurity threats. Both classified and unclassified indicators are reviewed and approved by CS&C in accordance with its written procedures. These

procedures include validating the indicators to ensure they are active, useful, and within policy before they are provided to the ISPs. Once an indicator is identified to be a viable indicator of a cyber threat, it will be used by CS&C and participating ISPs to detect malicious cyber activity. As a part of its indicator validation processes, CS&C assesses the quality of each indicator itself to determine whether there is a likelihood of false positives. CS&C cybersecurity analysts examine and evaluate all of the results to identify the true positives. The false positive results are of no value to the analysts and are purged according to established CS&C SOPs. CS&C and the ISPs then monitor the production environment to verify expected results. When a signature for a known or suspected cyber threat triggers an alert, that data is captured along with a predetermined amount of traffic that is analytically relevant to that particular threat.

E^{3}A will be deployed to identify and prevent known or suspected cyber threats against participating federal department and agency networks. As part of the E^{3}A process, ISPs may collect data directly related to an indicator discovered within monitored .gov traffic and that may contain information that could be considered PII.[13]

DHS uses the phrase "information that could be considered PII" because certain indicators of a cyber threat can be the same type of information individuals use to identify themselves in online communications such as an email address or other information that might be included in the message or subject line. In the context of E^{3}A, these types of information are not used to identify an individual; instead, they are used as a reference point for particular known or suspected cyber threats. For example, if the author of a cyber threat chose to use a fraudulent email address in the "from" field in a phishing email threat,[14] an indicator may be developed in response to that cyber threat that would include the email address. In this example, E^{3}A is not using the email address as PII, or even as general information about any specific person, it is simply using the information as an indicator of a potential cyber threat. DHS is only using this information to better identify a known or suspected cyber threat against computer networks. DHS may establish indicators with information that could be considered PII, but only if the information has proven to be analytically relevant to known or suspected cyber threats. The data is not used to identify specific individuals, nor are records searched by information that could be considered PII.

In situations when an indicator contains information that could be considered PII, DHS will follow defined SOPs and cybersecurity information handling guidelines, which specify procedures for handling sensitive information, including information that could

[13] The DHS Privacy Office Official Guidance defines PII as information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. Citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

[14] The Melissa virus (http://www.cert.org/advisories/CA-1999-04.html) propagates in the form of an email message containing malicious code as an attachment.

be considered PII. CS&C SOPs and information handling guidelines require CS&C cybersecurity analysts to minimize (i.e., overwrite, redact, or replace) PII data that is not necessary to understand the cyber threat. Specifically, the SOPs and information handling guidelines require CS&C cybersecurity analysts to screen all data and information that they intend to use to determine whether the information contains PII. If PII is discovered by CS&C cybersecurity analysts and is determined by the cybersecurity analysts to not be directly relevant to the cyber threat being analyzed, the information will be handled or minimized (replaced with a generic label as PII or deleted) by the cybersecurity analysts in accordance with CS&C SOPs and information handling guidelines.

CS&C requires the ability to perform deep packet inspection of known or suspected cyber threats that are identified by EINSTEIN sensors. CS&C screens all data captured by EINSTEIN 1 and EINSTEIN 2 sensors to ensure it is analytically relevant to a known or suspected cyber threat. E^{3}A combines existing analysis of EINSTEIN 1 and EINSTEIN 2 data as well as information provided by cyber mission partners with existing commercial intrusion prevention security services to allow for the near real-time deep packet inspection of federal network traffic to identify and react to known or suspected cyber threats. Network flow records contain only packet header information. Packet inspection tools allow an analyst to look at the content of the threat data, which enables a more comprehensive analysis. Packet Capture may contain information that could be considered PII-like malicious data from or associated with email messages or attachments. CS&C follows SOPs regarding handling of information that could be considered PII including the deletion of any PII unless there is a connection to a known or suspected cyber threat. Packet Capture shows details about the known or suspected cyber threat within the federal network. CS&C analyzes this detailed information and issues warnings, including possible mitigation strategies to the threat.

In accordance with the SOPs and information handling guidelines, all information that could be considered PII is reviewed prior to inclusion in any analytical product or other form of dissemination, and replaced with a generic label when possible. In some cases, a product may include information that could be considered PII because that information is deemed analytically relevant and necessary to understand the cyber threat. In those instances, the SOPs and information handling guidelines provide for safeguards regarding the marking, dissemination, and handling of the information.

Additionally, in order to evaluate the program and assess its compliance for the protection of PII and applicable laws and regulations, the NPPD senior privacy analyst conducts quarterly internal reviews of any PII retained, including descriptions of why it is necessary to retain the PII or verify its deletion.

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 following authorities permit and define the NCPS, E3A, and related EINSTEIN activities:

1) *Federal Information Security Management Act* (44 U.S.C § 3546) establishes that there will be a federal information incident security center, which will provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents; compile and analyze information about incidents that threaten information security; and inform operators of agency information systems about current and potential information security threats, and vulnerabilities. That center is US-CERT.

2) *Homeland Security Act of 2002 (*6 U.S.C. §§ 121 and 143) provides broad authority to DHS to access, receive, and disseminate information regarding threats to homeland security, including cybersecurity.

3) *Memorandum for Chief Information Officers, Office of Management and Budget Memorandum, M-06-19,* July 12, 2006, identifies US-CERT as the federal incident response center to which all federal agencies are required to report cybersecurity incidents.

4) *NSPD-54/HSPD 23*: *Comprehensive National Cybersecurity Initiative*, January 8, 2008, directs DHS to deploy intrusion detection and prevention sensors across federal civilian agencies[15].

5) *Office of Management and Budget (OMB) Memorandum: M-08-05, Implementation of Trusted Internet Connections (TIC),* November 20, 2007. This memorandum requires that all federal executive agencies use EINSTEIN 2 sensors.

6) *Memorandum for the Heads of Executive Departments and Agencies, Office of Management and Budget (OMB) Memorandum: M-10-28,* July 6, 2010, clarifies cybersecurity responsibilities and activities of the Executive Office of the President and the Department of Homeland Security (DHS); assigns

[15] For more information about The Comprehensive National Cybersecurity Initiative, see http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

to DHS responsibility for the operational aspects of federal civilian agency cybersecurity.

7) *National Strategy to Secure Cyberspace*, February 2003, recognizes DHS/US-CERT as the focal point for managing cyberspace incidents that could impact the federal government and national cyber infrastructures. The strategy also calls out five national priorities, three of which are addressed by CS&C: Securing Governments' Cyberspace, a National Cyberspace Security Awareness (and training) Program, and a National Cyberspace Security Response System.

8) *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure, including federal infrastructure. The Presidential Policy Directive allows the federal government to coordinate responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities.

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

Information regarding known or suspected cyber threats collected from federal departments and agencies, state, local, and tribal governments, industry, the general public, and international partners and collected through the NCPS and EINSTEIN is not based on data that identifies an individual but on the security event that triggered the alert. In the rare cases when E3A collects information that could be considered PII, this information is maintained and indexed by the security incident or cyber threat, not by the PII. CS&C does not maintain that information in a "system of records." As defined by the Privacy Act, a "system of records" is a group of any records under the control of any agency from which information is maintained and retrieved by a personal identifier. Only when there is actual retrieval of records by a personal identifier does the Privacy Act require a SORN. Because CS&C does not retrieve EINSTEIN information by a personal identifier, a SORN is not required.

The Privacy Act does not apply to information regarding known or suspected cyber threats. The Privacy Act does apply when PII may be used as an identifier for authorized users[16] that have been granted access to the NCPS or E3A (such as username or a government-issued email address). The Department of Homeland Security systems of records titled, DHS General Information Technology Access Account Records Systems

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

(GITAARS), September 29, 2009, 74 Fed. Reg. 49882, covers the collection of general contact and other related information used to grant access to employees, contractors and other individuals to the NCPS.

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

As part of the E3A effort, each ISP is required to provide DHS a system security plan that specifically documents its intrusion prevention security services implementation. As part of a DHS intrusion prevention security services security risk assessment process, this document is reviewed and approved by CS&C prior to production deployment of a service provider's intrusion prevention security services solution.

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

CS&C is currently working with the NPPD Records Manager to develop a disposition schedule that will cover all NCPS information.

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

Information is not being collected or solicited directly from the public; therefore, the Paperwork Reduction Act is not applicable in this situation. While information is being collected it is not done so through the solicitation of the same questions from 10 or more persons and in a manner that is consistent with PRA requirements.

Section 2.0 Characterization of the Information

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

E3A will entail commercial ISPs, under the direction of DHS, observing network and Internet traffic to or from participating agencies, traveling to or from a list of federal IP addresses provided by the agency and confirmed by both CS&C and their servicing ISP. The data associated with the observed federal network and Internet traffic, such as an email or an attachment, may include information that could be considered PII.

E3A ISPs perform pattern matching against established indicators based on known or suspected malicious traffic to or from the participating agencies. While the indicators will often be based on traffic metadata, such as IP addresses, they may potentially be

designed to match against any data in a packet, including the payload. Indicators are associated with a countermeasure to block malicious traffic to or from the participating agency.

CS&C uses analytically relevant EINSTEIN 1 and EINSTEIN 2 data to develop indicators created and validated by CS&C cybersecurity analysts through approved SOPs. These indicators are then shared with E3A ISPs.

All traffic associated with the supplied IP addresses for each agency is processed by the ISPs through the E3A technology. Agency traffic may contain information that could be considered PII. Indicators are only deployed in response to specific known or suspected cyber threats. Should a particular cyber threat include the use of information that could be considered PII, CS&C may deploy an indicator that uses that information or possibly a portion of the specific traffic as an indicator of that cyber threat in order to generate an alert or trigger a countermeasure. CS&C will deploy such indicators only for the purpose of detecting known or suspected cyber threats; CS&C will not deploy indicators that are intended solely to identify or collect PII.

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

The source of information analyzed by the ISPs will be federal network traffic to or from the participating agencies. This network traffic will be defined by the list of IP addresses supplied by each agency and verified by DHS and their E3A-servicing ISP.

Indicators and other cyber threat related information are received by CS&C from a number of sources including the following: analysis by CS&C's operations teams; data submitted to CS&C from other government departments and agencies; reports received from mission and industry partners; and commercially available cyber threat data feeds.

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

CS&C cybersecurity analysts use information from a range of sources, including commercial sources and publicly available data on cybersecurity threats (e.g., anything that could be found through open source Internet searches, newspaper articles). This data is used to understand cyber events that are reported to CS&C and for historical reference of similar incidents.

E3A does not use commercial or publicly available data for the purpose of identifying individuals. E3A uses indicators based on known or suspected malicious behavior. E3A may use indicators already identified by ISPs with the express approval of CS&C. E3A indicators may be derived from the same public sources referred to in the

NCPS PIA. Any data obtained from commercial sources is limited to information relevant to the DHS cybersecurity mission to protect the government network.

2.4 Discuss how accuracy of the data is ensured.

When federal agencies identify IP addresses associated with their networks, CS&C contacts the agency point of contact to verify the information. CS&C then provides the verified IP addresses to the ISPs. Following their own verification of the IP addresses as participating agencies that they service, the ISPs only analyze traffic associated with those IP addresses.

Contracts, service level agreements, and information handling procedures contain provisions to address circumstances in which an ISP detects network traffic that is not associated with a participating agency's network.

Both classified and unclassified indicators are reviewed and approved by CS&C in accordance with its written procedures. These procedures include validating the indicators to ensure they are active, useful, and within policy before they are provided to the ISPs. CS&C and the ISPs then monitor the production environment to verify expected results.

Verifying the accuracy of data for other components of the NCPS is addressed in the publicly available NCPS PIA.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: E3A may analyze, quarantine, store, or maintain more data than is necessary to address cybersecurity threats due to the nature of how the data is collected.

Mitigation: In order to limit the risk that too much network traffic will be analyzed, quarantined, stored, or maintained by the E3A ISP, participating agencies identify a list of IP addresses for their networks and both CS&C cybersecurity analysts and the ISPs verify the accuracy of the list of IP addresses provided by the agency. CS&C and the ISPs perform monitoring to identify any traffic that may be outside the range of identified IP addresses. In the event any out-of-range network traffic is identified, the ISP removes any collected data and prevents any further collection of this network traffic. To further limit this risk, CS&C reviews and approves all indicators that are provided to the ISPs to ensure that the corresponding signatures are tailored to only alert and mitigate traffic associated with cybersecurity threats. Additionally, CS&C has established a process through its contracts with the ISPs that gives CS&C the ability to review and approve all signatures associated with CS&C provided cyber threat indicators. Lastly, CS&C has defined the analytics requirements necessary to address a cybersecurity threat before submitting a request for a signature, which defines the analytic process for

determining whether or not a signature is needed. Following this process reduces the risk of collecting PII or information that could be considered PII and reduces the chance of analyzing, quarantining, storing, or maintaining more data than is necessary to address cybersecurity threats.

Privacy Risk: E^{3}A may collect information from network traffic that could be considered PII that may be inaccurate and/or malicious, for example a cyber threat may include an individual's email address.

Mitigation: As part of E^{3}A, CS&C uses information that is generated through EINSTEIN 1 and 2, which is described in the NCPS and EINSTEIN related PIAs, to generate indicators. Handling of all data is performed with applicable privacy protection mechanisms. Any information that is shared with CS&C by external partners that contains information that could be considered PII is handled in accordance with CS&C SOPs and information handling guidelines for handling sensitive information. Specifically, all information that could be considered PII is reviewed prior to inclusion in any analytical product or other form of dissemination, and replaced with a generic label (i.e., minimized) when possible – in accordance with established CS&C SOPs and information handling guidelines. In some cases, a product may include information that could be considered PII because that information is deemed analytically relevant and necessary to understand the cyber threat. In those instances, CS&C SOPs and information handling guidelines provide for safeguards regarding the marking, dissemination, and handling of the information.

ISPs view and analyze federal network traffic that is already available to them through existing agreements with participating agencies in order to apply indicators. Potential collection of network traffic is limited to the explicit purpose of identifying cyber threats. ISPs receive copies of established CS&C guidelines and SOPs regarding the handling and minimization of PII and the identification of sensitive information that may contain PII. Failure to meet these guidelines will be addressed through appropriate corrective action as defined by contract.

Privacy Risk: There is a risk that CS&C may use some information that could be considered PII in the development of cyber threat indicators.

Mitigation: CS&C adheres to strict procedures when creating indicators that may use information that could be considered PII, such as an email address or other information that might be included in the message or subject line. E^{3}A, and therefore CS&C, is not using the email address as PII, or even as information generally about any specific person. CS&C is only using this information to better define a known or suspected cyber threat against computer networks. CS&C does recognize that these types of indicators (i.e., spoofed or malicious email addresses) can, in other situations, be considered PII because it could be associated with a specific person; however, CS&C

does not use the PII for making this association. CS&C establishes indicators with information that could be considered PII only if analytically relevant to known or suspected cyber threats. Indicators for transmission to ISPs to support E3A are written and validated by CS&C cybersecurity analysts based on indicators of known or suspected cyber threats that are identified and validated by CS&C.

The privacy risk is additionally mitigated by limiting how the intrusion detection information is viewed. EINSTEIN data captured for CS&C use in developing indicators is only accessed by CS&C cybersecurity analysts with authorized access to NCPS systems.

Privacy Risk: There is a risk that information that could be considered PII is included in an indicator when that information does not add any value to the prevention of a known or suspected cyber threat.

Mitigation: CS&C only collects data that is necessary to accomplish its mission; cyber threat (i.e., indicator) information may include IP and host addresses and flow data, and any actions taken. CS&C cybersecurity analysts attempt to confirm the accuracy and integrity of the data received. Only information determined to be directly relevant and necessary to accomplish the specific purposes of the program is retained; otherwise, the data is deleted.

CS&C conducts periodic reviews on cyber indicators to ensure all standards and responsibilities are met and that the indicator is still operationally relevant.

Privacy Risk: There is a risk that the indicator is shared to the detriment of individuals who communicate electronically with the users' organizations or agency.

Mitigation: CS&C has established a process by which only trained and authorized users have access to the indicators. Users must abide by specific rules of behaviors and responsibilities with regard to access and to the quality of the data in NCPS systems. CS&C cybersecurity analysts conduct analysis on all cyber threats received. If a threat submitted contains information that could be considered PII, the analyst must determine if that information is directly relevant to the cyber threat. Any information that is not directly relevant to the cyber threat is deleted in accordance with CS&C information handling guidelines and SOPs.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

E3A includes the following to address managed security services and threat-based decision making:

- Indicators. Indicators are used in the IDS components of the E3A technology. All indicators are vetted through trusted and validated sources, using unclassified references for indicators whenever possible. The indicators are validated to ensure they are active, useful, and within policy before they are provided to the ISPs. These indicators are used to detect and respond to cybersecurity-related cyber threats within federal agencies' traffic. All indicators are reviewed and approved by CS&C in accordance with its written procedures.
- Intrusion prevention security capabilities. E3A includes a commercially available intrusion prevention security capability provided by ISPs that deploys countermeasures intended to block packets within traffic to or from federal agencies in order to counter known or suspected cyber threats that have been identified through indicators. The intrusion prevention security capability monitors traffic to or from participating agencies, in real time, for specific pre-defined cyber threats. When a specific threat is detected, the deployed E3A countermeasure may automatically block packets transiting to or from agency networks to counter the cyber threats. All countermeasures are reviewed and approved by CS&C prior to deployment in accordance with its written procedures. When an ISP implements signatures on behalf of DHS from information shared through indicators, and that signature triggers an alert, the ISP reports both the fact of occurrence and any additional details regarding the incident to DHS. ISPs also provide summary reports of intrusion prevention security activity to CS&C on a periodic basis.

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.

Yes. As described in this PIA, E3A provides query and analytical capabilities of its own data in order to fulfill the mission requirement. Queries are limited to cyber threat data and indicator information necessary to identify trends and patterns within cyber threat indicators and disparate data sets. CS&C cybersecurity analysts use cyber threat data to develop additional indicator information to be shared with E3A ISPs to integrate into their intrusion prevention security capabilities.

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

Only CS&C cybersecurity analysts and NCPS system administrators have access to the components of the NCPS system used for analysis and reporting. All E3A and

NCPS systems are governed by principles of least privilege that allow for limited views of data and rights to process information within E3A and the NCPS. For a full discussion of assigned roles and responsibilities within DHS and the NCPS, see the NCPS PIA.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that PII inadvertently obtained will be used inappropriately.

Mitigation: ISPs are restricted from using information that could be considered PII not directly related to an indicator as part of their deployment of intrusion prevention security services, nor for purposes beyond those specified by CS&C in support of E3A. As contractors to CS&C, the ISPs are required to conduct their activities in accordance with DHS requirements, including privacy training.

In addition, CS&C cybersecurity analysts as well as NCPS administrators and information assurance personnel are trained on both DHS and CS&C specific procedures for handling and safeguarding PII. CS&C cybersecurity analysts, administrators, and information assurance personnel received training upon hire, and are required to take refresher training each year on Security Education and Awareness Training (SEAT). In addition, CS&C maintains guidelines and SOPs for the purpose of identifying sensitive information, and for the proper handling and minimization of PII, to provide guidance for the necessary procedures and to define the terms of use for specifically identified roles and responsibilities.

Also, access to the NCPS and E3A is restricted to government and contractor staff with demonstrated need for access, and such access must be approved by the supervisor as well as the CS&C Information System Security Manager (ISSM). Authorized users must sign Rules of Behavior that identify the need to protect PII prior to gaining access. NCPS users' actions are logged and they are aware of that condition. Failure to abide by the Rules of Behavior may result in disciplinary measures and potential termination of employment.

Section 4.0 Notice

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

Notice is provided by privacy policies on an agency's website. In the individual MOA with DHS, the participating agencies are required to review any applicable external privacy policies to determine whether such policies should be revised to include notice of the deployment of EINSTEIN capabilities. Participating agencies are also required to provide log-on banners or notices, terms of use policies or user agreements, computer

training programs, or other mechanisms to notify federal agency computer users that the government routinely monitors communications occurring on agency networks for purposes including network operations, employee misconduct, law enforcement, and counterintelligence investigations. The notice also states that the government may – for any lawful government purpose – monitor, intercept, search, and seize any communications stored on or transiting to and from agency networks; and that communications or data may be disclosed or used for any lawful government purpose.

This PIA and the NCPS PIA serve as a general notice to individuals that network traffic flowing to or from participating federal civilian Executive Branch agencies may be collected for computer security purposes.

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

All authorized users logging into their participating agency's IT systems are presented with an electronic notice or banner that notifies them that government computer systems are monitored. Notice may also be provided on participating agencies public facing website privacy policies and through links from those policies, via the DHS Privacy Office and Cybersecurity privacy webpage. The participating agency website privacy policy states that the agency uses computer security programs to monitor network traffic. Authorized users inside the agency network receive notice by their agency's use of logon banners and user agreements notifying agency personnel that their communications or data transiting are stored on the agency network and that network traffic is subject to monitoring and disclosure for network security and other lawful government purposes.

Once an individual decides to communicate with a participating agency electronically, the network traffic is subject to computer security efforts of CS&C, including in this case E^{3}A, in addition to any individual computer security programs the agency might have in place.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that a person may not understand or read this PIA (or the participating agency's website privacy policy) to be aware of the information collection occurring under its computer security program or E^{3}A.

Mitigation: DHS provides a variety of notice mechanisms to authorized users of government systems both inside and outside the agency. The participating agency's website privacy policy states that the agency uses computer security programs to monitor network traffic. Authorized users inside the agency networks receive notice by the agency's use of logon banners and user agreements notifying agency personnel that their

communications or data transmissions are stored on their agency's network and that network traffic is subject to monitoring and disclosure for network security and other lawful government purposes. Individuals may also access the existing publicly available NCPS and EINSTEIN related PIAs or visit the DHS Privacy website that also provides resources explaining the DHS cybersecurity mission and programs.

Privacy Risk: There is a privacy risk that electronic communications between an individual and an agency may be interrupted by E3A's intrusion prevention security IPS capability, without notice to the individual.

Mitigation: DHS mitigates this risk as outlined above. In addition, this risk is mitigated through CS&C's written procedures that require CS&C to determine that a proposed countermeasure is narrowly tailored to take only those steps necessary to detect, analyze, respond to, or prevent known or suspected cyber threat. Countermeasures are also tested prior to implementation to ensure that any live traffic not indicative of a known or suspected cyber threat is not adversely affected. Refer to Section 3.1 for additional information on countermeasures. Lastly, the email quarantine capability allows for improperly quarantined messages to be released, further mitigating this risk.

Section 5.0 Data Retention by the project

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

The Department is currently working with the NPPD Records Manager to develop disposition schedules that will cover data collected and maintained under the NCPS, including E3A. Once completed, the schedule will be sent to the National Archives Records Administration for approval.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that PII may be inadvertently collected and retained beyond what is necessary to appropriately analyze or address a cyber threat or investigation.

Mitigation: As noted in the NCPS PIA, CS&C is currently working to determine the appropriate length of time for cyber indicators and related information, including information that could be considered PII and identified as related to a known or suspected cyber threat to be retained and stored. Data obtained by CS&C and the ISPs in the course of E3A will be maintained for the minimum time necessary.

Email traffic that is suspected of containing malicious attachments, URLs, and other forms of malware may be quarantined or redirected for further inspection. Quarantined email will be held for no more than 30 days.

CS&C cybersecurity 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 SOPs provide the procedures for marking and handling of PII collected as well as handling and dissemination instructions.

Section 6.0 Information Sharing

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

Participating agencies currently have access to their network flow records through participation in EINSTEIN 1 and receive information about their own data specific to their networks in accordance with CS&C's cybersecurity information handling policies and guidelines. Agencies are given access to information regarding their Agency network traffic that is being monitored and maintained within E3A. The access to the data is managed by CS&C. Depending on the ISP implementation of the service, the access may either be granted by CS&C to allow the Agency to access a particular data store within the ISP infrastructure (e.g., email quarantine server) or reports that capture and summarize suspicious or malicious cyber threat activity are sent directly to Agencies regarding their Agency's traffic.

Information collected, analyzed, or otherwise obtained by CS&C in connection with known or suspected cybersecurity threats or cyber incidents may be disclosed as part of their work products in furtherance of the DHS cybersecurity mission to protect federal information systems from cybersecurity threats and to mitigate against such threats, or respond to a cyber incident in accordance with the cybersecurity information handling policies and guidelines.

CS&C shares analysis, along with additional computer network security products, with its partners and constituents (federal departments and agencies, state, local, and tribal governments, industry, academia, and the general public and international partners) via its web site: www.us-cert.gov.

For additional information on information sharing, see the NCPS PIA. Contact information from representatives of the participating ISPs, and federal civilian Executive Branch agencies will not be shared outside of normal agency or E3A operations.

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

Information regarding known or suspected cyber threats collected from federal departments and agencies, state, local, and tribal governments, industry, the general public, and international partners and collected by the NCPS and EINSTEIN (EINSTEIN 1, EINSTEIN 2, and E3A), is not based on data that identifies an individual but on the security event that triggered the alert. As defined by the Privacy Act, a "system of records" is a group of any records under the control of any agency from which information is maintained and retrieved by a personal identifier. Only when there is actual retrieval of records by a personal identifier does the Privacy Act require a SORN. Because CS&C does not retrieve NCPS and EINSTEIN information by a personal identifier, a SORN is not required.

The Department of Homeland Security systems of records titled, DHS General Information Technology Access Account Records Systems (GITAARS), September 29, 2009, 74 Fed. Reg. 49882, covers the collection of general contact and other related information used to grant access to employees, contractors and other individuals to the NCPS. This collection is also covered under the existing NCPS PIA. CS&C will share this data in a manner that is compatible with the purpose of the aforementioned systems of records notice.

6.3 Does the project place limitations on re-dissemination?

Cyber threat information received through E3A or other means is reviewed to determine if it contains information that could be considered PII and if so, that information is reviewed and only disseminated if sharing the actual information is analytically relevant to the cyber threat. If PII needs to be disseminated 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.

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.

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 incident or series of incidents 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. [17]

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: If non-cybersecurity information must be shared outside of DHS, it increases the risk of unauthorized disclosure.

Mitigation: Information about known or suspected cyber threats collected, analyzed, or otherwise obtained by CS&C may be disclosed for cybersecurity purposes and in furtherance of the DHS cybersecurity mission.

Information collected by E3A or otherwise obtained by CS&C may be disseminated for non-cybersecurity purposes in limited situations when the collected information appears to indicate involvement in activities that may violate laws or otherwise when the sharing is done in the performance of a lawful government function. This may include dissemination for law enforcement/intelligence or administrative purposes unrelated to the protection of an information system from cybersecurity threats, mitigations against such threats, or response to a cyber incident. In such cases, the recipient will be a federal, state, or local law enforcement entity.

Only information that is necessary to understand reports will be included in any of these products. When such authorized dissemination includes information associated with a specific individual or information that could be considered PII, dissemination will comply with the requirement of SOPs and established cybersecurity information handling guidelines. Any dissemination of information for non-cybersecurity purposes must also be approved by CS&C leadership pursuant to guidance from the DHS Office of General Counsel.

Appropriate instructions for marking and handling are provided as part of the SOPs about handling data for further dissemination. SOPs require that reports with information that could be considered PII include markings for the first reference to each instance of the PII. If the report is modified for multiple audiences, each version is reviewed for appropriate markings. Handling and dissemination instructions are also included in the SOPs and information identifying sources and methods from all CS&C reports and products are required to be redacted prior to dissemination.

Unauthorized disclosure is mitigated through various means, including encrypting information and limiting distribution of the information. The E3A-Mission Operating Environment that supports the E3A implementation has been engineered specifically to prevent both unauthorized entry as well as unauthorized exfiltration of data.

[17] Approval is not required when information about a specific person is believed to be fictitious, when the information is publicly available, or when the release of such information is being coordinated with the person with whom it is associated.

Section 7.0 Redress

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

Information regarding known or suspected cyber threats collected from federal departments and agencies, state, local, and tribal governments, industry, the general public, and international partners and collected by the NCPS and EINSTEIN, is not based on data that identifies an individual but on the security event that triggered the alert. E3A does not change the opportunities for access, redress, or correction under the NCPS.

Individuals seeking access to any record containing information that is part of a DHS system of records, or seeking to amend the accuracy of its content may submit a Freedom of Information Act (FOIA) or Privacy Act (PA) request to the DHS/NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380. Individuals may obtain directions on how to submit a FOIA/PA request at http://www.dhs.gov/xfoia/editorial_0316.shtm.

The release of information is subject to standard FOIA Exemptions. Given the nature of the cyber threat information contained in E3A and NCPS, CS&C may not always permit individuals to gain access or grant request for amendment of their record(s). Records, as defined by the Privacy Act, would only consist of log-in/contact information covered under the GITAARS SORN.

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

E3A does not change the procedures previously published in the NCPS and EINSTEIN-related PIAs.

There are no separate procedures for individual correction of information collected by sensors since flow records, alerts, and associated indicators are generated from exact copies of computer network traffic. This is consistent with the previously published NCPS and EINSTEIN-related PIAs.

An individual can submit a written request to DHS/NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380, to have their inaccurate or erroneous PII corrected. See additional information in Section 7.1.

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

E3A does not change the procedures previously published in the NCPS and EINSTEIN-related PIAs. Under E3A, as with the NCPS, an individual can still submit a written request to DHS/NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C.

20528-0380, to update their log-in/contact information. See additional information in Section 7.1.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will want to seek redress procedures for data associated with a known or suspected cyber threat.

Mitigation: Additional redress procedures beyond those described above are not available because information collected as part of the NCPS and EINSTEIN is not based on data that identifies an individual but instead on the security event that triggered the alert. ISPs use E3A to analyze traffic and create reports based on indicators, not by PII. The security event that triggered the alert is how data is retrieved, stored, and reported. As such, there is no information about an individual that can be used to access the cybersecurity threat or event(s).

Section 8.0 Auditing and Accountability

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

E3A follows the same procedures as previously identified and published in the NCPS PIA.

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

The training provided to federal and contracted DHS users is articulated in the NCPS PIA. As contractors to CS&C, ISPs must comply with established CS&C guidelines and SOPs regarding the handling and minimization of personally identifiable information and the identification of sensitive information that may contain personally identifiable information.

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

CS&C users must obtain a favorable DHS suitability determination[18] prior to acquiring access to certain NCPS systems.

[18] The suitability determination is a process that evaluates federal or contractor employees' personal conduct throughout their careers. Suitability refers to fitness for employment or continued employment referring to identifiable character traits and past conduct that is sufficient to determine whether or not an individual is likely to carry out the duties of the position with efficiency, effectiveness, and in the best interests of the agency.

All authorized users accessing classified information and technology must be cleared to access that specific information or technology as well as maintain the general standards required to hold the security clearance. All NCPS users supporting the program have a valid requirement to access the systems and only the type of access required to meet their professional responsibilities. Access is based upon the role identified on their access requests form (i.e., analyst, user, general user, system administrator, network administrator). The NCPS access form must be completed by the government supervisor within the branch that the authorized user will be supporting. The user's role is defined by the branch manager and validated by the ISSM. Accounts are reviewed monthly by the ISSM to ensure that accounts are maintained current. In addition, user account activity is logged, and the logs are reviewed daily.

In addition, CS&C maintains SOPs on privacy protection for the purpose of identifying sensitive information, and for the proper handling and minimization of PII. The SOPs outline the necessary procedures and define the terms for specifically identified roles and responsibilities. These SOPs are provided to CS&C cybersecurity analysts and NCPS system and network administrators so that they are aware of what information should and should not be shared with its information sharing partners. Specific SOPs for PII handling and minimization are also shared with the ISPs.

All authorized CS&C users of the E^3A system must complete a review and acknowledgement of the NCPS rules of behavior prior to gaining access to the system. CS&C requires ISPs to define a concept of operations that documents their internal system guidelines and procedures, to include supporting SOPs.

Agencies are given access to information regarding their agency network traffic that is being monitored and maintained within E^3A. The access to the data is managed by CS&C. Depending on the ISP implementation of the service, access may be granted by CS&C to allow the agency to access a particular data store within the ISP infrastructure (e.g., email quarantine server) or reports that capture and summarize suspicious or malicious cyber threat activity are sent directly to agencies regarding their agency's traffic.

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

The MOAs developed between DHS and other federal departments and agencies are based on an approved template that has been fully coordinated through the program manager, system owner, Office of the General Counsel, and the NPPD Office of Privacy. New uses of the information and new access to the system by organizations within DHS and outside are similarly reviewed by various stakeholders, including integrated program teams with approval vetted through upper management.

Responsible Officials

Brendan Goode
Director, Network Security Deployment
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security