Privacy Impact Assessment
for the

National Cybersecurity Protection System (NCPS)

DHS/NPPD/PIA-026

July 30, 2012

Contact Point
Brendan Goode
Director, Network Security Deployment
National Cyber Security Division
National Protection and Programs Directorate
Department of Homeland Security
(703) 235-2853

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The National Cybersecurity Protection System (NCPS) is an integrated system for intrusion detection, analysis, intrusion prevention, and information sharing capabilities that are used to defend the federal civilian government's information technology infrastructure from cyber threats. The NCPS includes the hardware, software, supporting processes, training, and services that are developed and acquired to support its mission. The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), National Cyber Security Division (NCSD) is conducting this Privacy Impact Assessment (PIA) because personally identifiable information (PII) may be collected by the NCPS, or through submissions of known or suspected cyber threats received by the United States–Computer Emergency Readiness Team (US-CERT) for analysis. This PIA will serve as a replacement for previously published PIAs submitted by NSCD for the 24/7 Incident Handling Center (March 29, 2007), and the Malware Lab Network (May 4, 2010), and is a program-focused PIA to better characterize the efforts of NCPS and US-CERT.

Overview

The federal government relies on its information technology (IT) infrastructure and the Internet to provide efficient and effective services to manage the growing amount of data needed to carry out its missions. This reliance makes the federal IT infrastructure a high-priority target for sophisticated adversaries.

In order to face these adversaries, the Department of Homeland Security (DHS) maintains an organization to serve as the focal point for security of cyber infrastructure and to facilitate interactions between and among federal departments and agencies (D/A), state and local governments, public and private sector Critical Infrastructure/Key Resources (CI/KR), and international organizations. The organization responsible is the National Cyber Security Division (NCSD). See Appendix for an acronym list.

Organizations within NCSD

In 2008, in response to expanding cybersecurity mission requirements from Congress and the Administration, NCSD established the NCPS to protect the federal civilian government network and prevent known or suspected cyber threats. The Network Security Deployment (NSD) branch of NCSD 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 NCSD branches to ensure that NCPS capabilities deployed by NSD support and augment the mission capabilities of those branches (as applicable).

The NCPS provides the technical foundation for US-CERT activities. US-CERT is the primary user of NCPS capabilities[1] and works to protect and defend the nation's cyber infrastructure. US-CERT is the front line against cyber threats and works to collect and disseminate cybersecurity threat information. During the collection and analysis of data related to known or suspected cyber threats, US-CERT may collect or discover information that could be considered PII. US-CERT follows strict standard operating procedures (SOPs) regarding this collection and only keeps PII if it relates to a known or suspected cyber threat; if there is no connection, the PII is deleted.

The remaining three NCSD branches – Federal Network Security (FNS), Global Cyber Security Management (GCSM), and Critical Infrastructure Cyber Protection and Awareness (CICPA) – benefit from the information collected and produced by US-CERT analysts and may use US-CERT's analysis of NCPS data as well as the NCPS information sharing capability to meet their mission needs.

NCSD's FNS branch identifies risks to the federal enterprise and shapes federal policy regarding solutions and services for federal IT systems. FNS also coordinates internal security, compliance, and agency implementation of strategies for NCSD. Within DHS, FNS administers the Federal Information Security Management Act[2] (FISMA) reporting of federal executive civilian branch agencies. These FISMA reporting responsibilities are met with the NCPS CyberScope[3] capability, which is administered by NSD. NSD and FNS also coordinate closely to ensure cybersecurity policies, initiatives, standards, and guidelines for implementation across the federal civilian government are in harmony with the technical and mission needs of the NCPS throughout its development and implementation.

NCSD's GCSM branch directs policy, long-term strategy, and analysis for the nation's CI/KR. GCSM's mission is to promote cybersecurity of the nation's CI/KR by developing and disseminating sound practices for software developers, information technology security professionals, and other cybersecurity stakeholders that address strategic and long-term cyber issues including security of the supply chain, developing the cybersecurity workforce, and building security into software. GCSM may leverage US-CERT analyses and post-analysis of NCPS data to identify vulnerable areas of the system in order to conduct trend analysis and determine threat behavior, and to identify system vulnerability points in order to develop mitigation and prevention strategies for

[1] Aside from the information sharing capability, the other NCSD branches do not directly access data received or input into the NCPS. However, NCPS capabilities could use the information or analysis that is produced from the data collected via other NCSD organizational authorities. For example, Federal Network's Security's continuous monitoring mission will eventually feed into the NCPS.

[2] FISMA is the Federal Information Security Management Act of 2002. It was passed as Title III of the E-Government Act (Public Law 107-347) in December 2002. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

[3] CyberScope is a web-based tool DHS uses to track FISMA requirements from all federal Departments and Agencies.

future systems. GCSM will also leverage NCPS information sharing capabilities to share the national cybersecurity knowledgebase to enable success against current and future cyber threats.[4]

Finally, NCSD's CICPA branch provides federal government assistance in cyber protection to the nation's CI/KR. CICPA also evaluates and assesses CI/KR capabilities by launching cyber exercises to test both individual sector vulnerabilities and response to the overall federal and partner responses to larger scale incidents. CICPA works closely with US-CERT in situations where an event or identified risk could have an impact on the critical infrastructure and will leverage NCPS information sharing capabilities to extend its cyber expertise to sector specific working groups and Information Sharing and Analysis Centers (ISACs).[5]

NCPS Capabilities

The NCPS is a suite of capabilities that monitor and analyze cyber threat data transiting to and from federal civilian government networks. These capabilities are described in detail below:

- Core Infrastructure
  - Mission Operating Environment (MOE)
  - EINSTEIN 3 Accelerated (E^3A) Mission Operating Environment (E^3A-MOE)
  - Incident Management System (IMS)
  - Development & Test (Dev/Test) Environment
- Intrusion Detection
  - EINSTEIN 1
  - EINSTEIN 2
  - Passive Domain Name System (pDNS)
- Analysis
  - Packet Capture (PCAP)
  - Security Information and Event Management (SIEM)
  - Enhanced Analytical Database (EADB) and Flow Visualization

[4] NSD will also benefit from the standards development work that GCSM engages in as the NCPS will eventually employ those standards.

[5] In response to meeting the specific goals, objectives, and requirements of the Homeland Security Presidential Directive (HSPD)-7, Information Sharing and Analysis Centers (ISAC) are private sector operational organizations that have been established to collect, distribute, analyze, and share sensitive information regarding threats, vulnerabilities, alerts, and best practices in order to protect the national critical infrastructures of North America in the chemical, electrical, energy, financial services, healthcare, information technology, public transit, surface transportation, telecommunications, truck, and water sectors. Together to advance the physical and cyber security, they create an ISAC Council, partnering with their sectors, with one another, and with government.

- Advanced Malware Analysis Center (AMAC)
- Digital Media Analysis Environment (Forensics)

- Information Sharing
  - CyberScope
  - US-CERT.gov Website and US-CERT Portal
  - Cyber Indicators Repository (CIR)
  - Cyber Indicators Analysis Platform (CIAP); and
- Intrusion Prevention
  - EINSTEIN 3 Accelerated (E^3A)

Core Infrastructure

Mission Operating Environment (MOE)

The MOE is a dedicated network environment upon which NCPS intrusion detection, intrusion prevention, analysis, and information sharing capabilities are hosted. The MOE is the infrastructure for the NCPS; it is the communications network and operating system, used exclusively by US-CERT to conduct its daily operations.[6] As a dedicated network environment, the MOE allows US-CERT to protect its core operations in addition to providing cross-agency infrastructure assurance and cybersecurity services. US-CERT analysts may receive suspicious files, spam, and other potential cyber threats via an email network, exclusively used within the MOE, some of which might contain PII. US-CERT conducts aggressive analysis of the items to determine the nature of the threat, source, intent, target, and mitigation. If the analyst determines that the PII does not relate to a known or suspected cyber threat; it is immediately deleted from the MOE.

As a closed communications network, the MOE is also used for issuing regular security and warning bulletins and receiving public contribution and outreach. The MOE might collect PII, such as contact information from those who contribute security alerts or those who receive warning bulletins. As a dedicated network, the MOE does not directly connect to any DHS networks to protect the Department from harm as a result of the type of information it may receive.

EINSTEIN 3 Accelerated-Mission Operating Environment (E^3A-MOE)

The E^3A-MOE provides a secure network environment, specifically designed to support unique NCPS intrusion prevention capabilities. Like its MOE counterpart, the E^3A-MOE serves as a dedicated communications network and operating system, used exclusively by US-CERT personnel that are specifically assigned to intrusion prevention cybersecurity services. The E^3A-MOE follows the same PII handling procedures as the MOE. If an analyst determines that the PII collected on the

[6] As the system developer and operator, NSD also uses the MOE to provide user support to US-CERT and to deploy and maintain NCPS capabilities.

E^3A-MOE does not relate to a known or suspected cyber threat, it is immediately deleted from the E^3A-MOE. The E^3A-MOE is a dedicated and isolated network and does not directly connect to any DHS networks or NCPS systems.

Incident Management System (IMS)

Individuals from the private and public sector may contact US-CERT on a 24/7 basis. The individual's contact information and the nature of the concern are collected and documented by the operations center personnel in the IMS. Once recorded, an incident is created and notification is sent to the appropriate section within US-CERT to be handled.

When an incident has been reported, a follow-up assessment of the incident and the event is conducted within the operations center. In some cases, incidents are assigned to specific groups outside of the operations center, such as the Digital Media Analysis team, the Code Analysis team, the EINSTEIN team, or they are assigned to the Senior Watch Officer on duty. As an example, the Code Analysis team within US-CERT may be assigned incidents that involve malware analysis. The assigned team provides updates on its analysis and handling of the incident in the IMS.

In the course of daily operations, US-CERT will evaluate all incident reports or other forms of incoming communications, which are entered into the IMS, for possible relevance to the mission, primary jurisdiction, or other applicable authorities. As incidents of interest to law enforcement, counterintelligence, and counterterrorism or intelligence communities are reported to US-CERT, US-CERT follows SOPs to ensure that the necessary information is shared with the appropriate parties for action and collaborative efforts where possible. In the course of normal operations, it is possible that PII, beyond name and contact information, could be collected through the submission of a known or suspected cyber threat. If PII is collected, US-CERT follows SOPs that require an immediate review of the PII for its relevance to a known or suspected cyber threat and removal of any PII not related to a known or suspected cyber threat.

Development & Test Environment (Dev/Test)

The NCPS Dev/Test Environment provides a vehicle to test new capabilities under consideration for deployment, in a simulated end-to-end NCPS system prior to deployment to a production system, in order to mitigate potential vulnerabilities, and reduce impacts when transitioning to the operations.

In order to meet the strategic goals for the NCPS, NSD's engineering group uses the following strategic approach for the NCPS Dev/Test Environment:

- Seek to establish a unified approach for development of testing cyber-security services and capabilities;
- Simulate the current operational environment to include systems, connectivity, and capabilities;

- Identify the development and testing environment configurations needed to meet different project requirements;
- Identify requirements for development testing assets (i.e., hardware and software) plus human resources to meet long-term program requirements; and
- Allow interaction with end-user analyst (US-CERT) to:
  - Provide experience and training with new platforms/capabilities before they are deployed into production network;
  - Increase knowledge transfer to better support operations;
  - Demonstrate critical performance metrics, such as load and capacity and/or user interface; and
  - Establish an environment for showcasing rapid-prototypes as well as validating emergency repairs.

The NCPS Dev/Test Environment will use both synthetic data, as well as EINSTEIN 2 operational data that are more than 30 days old for test purposes, which will be stored within the NCPS Dev/Test Environment infrastructure. Since all PII contained in data sets will be anonymized as part of collection in EINSTEIN 2, all operational data that is used in the Dev/Test Environment will be sanitized prior to introduction into the environment. All data will be presented in such a way as to conceal any machine- or human-readable information and thus prevent the disclosure of security information or information that could be considered PII such as the Source Internet Protocol (SIP) address of the source computer involved in the data transaction as well as the Destination Internet Protocol (DIP). Upon conclusion of each test, the data will be deleted from the system being tested.

Specific technical, operational, and managerial controls are implemented to ensure a safe and appropriately secure environment necessary to provide functional capabilities for the development and testing of new tools.

The NCPS Dev/Test Environment uses approved and standardized data sets determined by the designated Information System Security Officer (ISSO) which are available to all NCPS capability development projects. The test environment does not contain DHS-sensitive information that merits special handling and will operate in a non-production environment throughout its lifecycle; any changes to this process will be evaluated for privacy implications and documented in an updated PIA as necessary. Access is limited to individuals who are required to sign rules of behavior regulating their actions when utilizing the test environment.

<u>Intrusion Detection</u>

The NCPS uses an integrated system of multiple capabilities to defend the federal civilian government's information technology infrastructure from cyber threats. Intrusion detection is a capability that alerts US-CERT to the presence of malicious or potentially harmful computer network activity in federal executive agencies' network traffic. Intrusion detection is deployed through the EINSTEIN system and provides for improved detection and notification capabilities to provide near real time response.

EINSTEIN 1

EINSTEIN 1, developed in 2003, provides an automated process for collecting computer network security information from voluntary participating federal executive agencies. It works by collecting network flow records.[7] DHS conducted a Privacy Impact Assessment on EINSTEIN 1 in 2004.[8]

Using network flow records, US-CERT can detect certain types of cyber threats (e.g., compromised systems or hosts) and coordinate with the appropriate federal executive agencies to mitigate those threats and vulnerabilities. US-CERT shares this analysis, along with additional computer network security information, as appropriate, with both the public and private sectors, via the US-CERT web site at www.us-cert.gov. FNS, GCSM, and CICPA may use US-CERT's analysis of EINSTEIN 1 data to develop standards or recommendations for their stakeholder communities.

EINSTEIN 2

EINSTEIN 2, like EINSTEIN 1, passively observes network traffic to and from participating federal executive agencies' networks. In addition, EINSTEIN 2 adds an intrusion detection system (IDS) capability that alerts when a pre-defined specific cyber threat is detected and provides the US-CERT with increased insight into the nature of that activity. Through EINSTEIN 2, US-CERT is able to analyze cyber threat activity occurring across the federal IT infrastructure resulting in improved computer network security situational awareness. This increased situational awareness can then be shared with individual federal executive agencies in an effort to reduce and prevent computer network vulnerabilities. DHS conducted a Privacy Impact Assessment on the EINSTEIN 2 in 2008.[9]

Similar to EINSTEIN 1, FNS, GCSM, and CICPA may leverage US-CERT's analysis of EINSTEIN 2 data. For example, GCSM may use US-CERT's analysis of an alert from EINSTEIN 2 to develop recommendations to better secure the supply chain. NSD coordinates with US-CERT to ensure that the deployed EINSTEIN 2 capability meets US-CERT's mission requirements.

EINSTEIN 2's network intrusion detection technology uses a set of custom signatures[10] based upon known or suspected cyber threats. Signatures are derived from numerous sources such

[7] "Flow records" are records of connections (source Internet Protocol (IP) address, destination IP address, time, port used and sent to) made to a federal executive agency's IT systems.

[8] Information on the EINSTEIN Program PIAs is available at the following link: http://www.dhs.gov/files/publications/gc_1284567214689.shtm

[9] Information on the EINSTEIN Program PIAs is available at the following link: http://www.dhs.gov/files/publications/gc_1284567214689.shtm

[10] 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.

as: commercial or public computer security information; incidents reported to US-CERT; information from federal partners; or, independent in-depth analysis by US-CERT analysts.

EINSTEIN 2 is not programmed to specifically collect or locate PII. While signatures might be developed in response to known or suspected cyber threats with indicators[11] containing information that could be considered PII, the purpose of these signatures is to prevent cyber threats from reaching federal networks, not to identify or collect PII. For example, if a computer security exploit chose to use information that could be considered PII in the delivery of malicious code, a signature could be developed in response to that exploit which could contain that information.[12] Accordingly, while EINSTEIN 2 will collect information that could be considered PII that is directly related to a cyber threat being transmitted to the federal networks, its main focus is to identify the cyber threat and protect federal networks, not to collect PII.

NCSD has a governance structure for the creation and review of signatures and a process by which the NCPS alerts US-CERT of a known or suspected cyber threat. The signature development process determines whether particular signatures will direct the capture of associated traffic and how much traffic must be collected based on the particular cyber threat in accordance with US-CERT written procedures and is subject to review by the Office of General Counsel, the US-CERT Oversight and Compliance Office, as well as the NPPD Office of Privacy. US-CERT will deploy signatures that use information that could be considered PII only if the signatures have been approved in accordance with written procedures and only for the purpose of detecting cyber threats.

EINSTEIN 2 only alerts US-CERT when the system identifies known or suspected cyber threats detected in traffic to or from a federal executive agency's network in response to specific custom signatures. A US-CERT analyst may then query that specific information on the sensor to analyze the potentially harmful network traffic identified by the alert. US-CERT analysts view only the specific intrusion detection information associated with the triggering alert. The intrusion detection information used by US-CERT is that portion of the network traffic that is analytically relevant to the specific known or suspected cyber threat identified in the specific signature.

EINSTEIN 2 is intended to augment – not replace or reduce – the current computer network security practices of participating federal executive agencies. Participating agencies continue to operate their own intrusion detection and prevention systems, perform network monitoring, and use other information security technologies. These sensors enable US-CERT to correlate activity across the participating federal executive branch agencies. With the enhanced correlation capability, US-CERT achieves increased situational awareness of high profile cyber threats which is required to perform the computer network security responsibilities assigned to DHS.

[11] A cyber indicator (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.

[12] For example, 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. That email message could contain PII.

Passive Domain Name System (pDNS)

While EINSTEIN 2 alerts when specific malicious network activity is detected, US-CERT also has a critical need for a capability to collect, query, and analyze the operationally relevant Domain Name System (DNS) data being generated by federal agencies. This need is resolved by utilizing pDNS.

Like the analysis of EINSTEIN 1 and 2 data, US-CERT's analysis of pDNS data would be useful to other organizations within NCSD, such as CICPA or GCSM. For example, the analysis may show that only electrical sector stations were being attacked instead of other utilities and CICPA could develop recommendations to better protect that sector.

Cyber threat actors rely heavily on controlling their network Command and Control infrastructure that is typically built on a DNS infrastructure. Failure to collect this machine-to-machine data and leverage the data for network forensic investigation creates a significant gap in the identification of cyber threats and cyber threat actors. The ability to collect, query, and historically track indicators of cyber threats allows US-CERT to better investigate known or suspected cyber threats against the federal network space.

Enabling the passive collection of DNS data is accomplished by activating a feature on the publicly-available "Yet Another Flowmeter" (YAF) software residing on EINSTEIN 1 sensors. Enabling the pDNS feature on YAF allows for the collection of all DNS traffic crossing the boundaries of the EINSTEIN monitoring sensors, thus providing US-CERT with a high level overview of all DNS traffic within the federally monitored space.

There are four types of information present in passive DNS collection:

1) DNS queries;

2) DNS records that are given in response to queries, i.e., positive answers;

3) Negative answers to queries; and

4) IP addresses associated with the systems asking and answering the queries.

DNS queries are contained in answers, so if all answers are captured there is no need to capture queries. If negative answers are not captured, but positive answers and queries are, the negative answers can be inferred from the queries.

The DNS records contained in positive answers is public by definition. They are given by name servers that are explicitly registered to provide this information to the public. These public answers are necessary for much of the Internet to function as we expect it to.

A large proportion of DNS queries are never answered and these queries are also of interest to cyber analysts. When analyzing pDNS data, distinguishing between positive answers and negative answers, i.e., demonstrations of non-existence, is an analytic objective. These unanswered queries do not contain inherently public information - since they are unanswered, their subject is not in the

DNS. Unanswered queries are often the result of misconfigurations somewhere on the network, which can inform a significant amount of network configuration information from the DNS data. This configuration information does not contain PII; however, it can be considered sensitive system configuration information. Malicious software on the network is also sometimes the source of these unanswered questions, and a sense of the malicious activity on the network can be obtained from these suspicious queries. It can also lead to further investigations to identify the infected machines and clean them.

Collecting IP addresses associated with the systems asking and answering queries (see above number 4) does not suggest that the end-user who issued the query can be identified. Due to the DNS protocol and implementation, the passive collection of DNS traffic (pDNS) is effectively prevented from collecting the identity of the querying entity. Since DNS queries are resolved hierarchically, the querying entity is naturally anonymized. Also, since the network address of the original querying entity is removed, the time of the original query is not precisely preserved, and most individual queries never reach the sensor, therefore, it is not possible to reconstruct any end-user identities from pDNS.

None of the domain names or IP addresses stored in the pDNS database contains PII that exceeds what is currently collected in the IMS (e.g., name, address, telephone number, email address, details about the reported incident). Any PII that is collected and determined not necessary to understand the analysis or product, will be minimized.[13] Any DNS record information containing PII that is relevant and necessary and retained for the purposes of analyzing or responding to an incident is retained and disposed of in accordance with the draft records schedule for the NCPS.

Analysis

The NCPS analysis capability provides US-CERT with the ability to compile and analyze information about known or suspected cyber threats and inform federal, state, and local government agencies; private sector partners and infrastructure owners and operators; and the public about current and potential cybersecurity threats and vulnerabilities. NCSD branches like FNS, GCSM, and CICPA may also leverage US-CERT's analysis to develop guidance or policy for federal agencies, CI/KR owners and operators, state, local, tribal, territorial government entities, and the supply chain, as applicable.

The NCPS analysis capability includes several tools to capture and analyze data, such as PCAP, SIEM, Forensics, and AMAC. These tools are needed to organize the data collected and produced by the NCPS. For example, PCAP allows US-CERT analysts to see "inside" the packet and inspect the payload to analyze a specific cyber threat, SIEM organizes threat data to support that analysis, and the malware capabilities will provide a mechanism by which information regarding cyber threats can be collected and contained in a highly secure environment to allow for analysis and

[13] PII in US-CERT data that is not relevant or necessary to understanding the cyber threat, shall be minimized, for example, any PII such as a name or email address that may be part of header or footer data of a cyber threat: "John.Doe@email.com" will be replaced with "PII".

evaluation of the threat by expert analysts to improve the overall understanding of current or emerging cyber threats.

Packet Capture (PCAP)

The NCPS needs the ability to perform deep packet inspection[14] of known or suspected cyber threats that are identified by EINSTEIN sensors. To this end, the NCPS maintains a PCAP environment that provides US-CERT analysts with the ability to inspect the PCAP payload information, transform JavaScript source code into a human-readable code so that US-CERT analysts can assess the script functionality and application, and assess the impact and effect of Botnet activity. PCAP may contain information that could be considered PII-like malicious data from or associated with email messages or attachments. NCSD 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.

The NCPS PCAP environment was designed as a "closed," virtualized environment to ensure protection for the MOE and any data at rest. The data at rest is protected by file encryption. All malicious code is contained within this protected PCAP environment.

Metadata derived from the PCAP analysis may contain email addresses and IP addresses. The capability to feed that metadata to another protected capability in the MOE may be developed to meet operational needs. Currently, the NCPS EADB is capable of accepting a feed of this metadata. The NCPS SIEM is the only other NCPS component that may be enhanced to accept a feed of this metadata. The SIEM and EADB have sufficient controls in place to protect the metadata. Any changes to current processes will be documented in an updated PIA.

The PCAP environment is configured to capture and store PCAP data associated with known or suspected cyber threats, i.e., events triggered by an EINSTEIN sensor or the SIEM. During packet collection, any packets older than 30 days and not deemed to be related to a cyber threat are purged from the environment's storage.

PCAP shows details about the known or suspected cyber threats within the federal network. US-CERT analyzes this detailed information and issues warnings including possible mitigation strategies to the threat.

Security Information and Event Management (SIEM)

The NCPS provides the SIEM capability to simplify cyber analysis by aggregating similar events (thus reducing duplication), correlating related events (that might otherwise go unnoticed), and providing visualization capabilities (making it easier to see relationships between events). The SIEM processes certain portions of data, collected from both EINSTEIN 1 and EINSTEIN 2, but

[14] Deep packet inspection means being able to look into the content of cyber traffic. Netflow data is just packet header information, which is limited. Packet inspection tools allow an analyst to look at the content of the threat data which enables more comprehensive analysis. Deep packet inspection is only performed in the PCAP environment.

does not process all of the data collected by those sensors. The portion of EINSTEIN 2 data that is currently analyzed by the SIEM does not include PII.

As the NCPS progresses it may be deemed necessary to provide longer-term storage and retrospective analysis of PCAP. If this is necessary, then the SIEM will be allowed to ingest and analyze PCAP data which might contain PII. If this capability is allowed, the SIEM has system controls in place to protect the PII including restricting access to only individuals with log-in and user accounts, encrypting all communications and not allowing external access to the data.

Enhanced Analytical Database and Flow Visualization (EADB)

The EADB system utilizes Commercial-Off-The-Shelf (COTS) technology that employs high speed massively parallel processing (MPP) and input/output (I/O) capabilities, which are supported by a large database storage capacity. The EADB is able to ingest various external data sources (e.g., threat sources, threat feeds, EINSTEIN 1 NetFlow, EINSTEIN 2 Intrusion Detection events, PCAP, etc.). The EADB then serves as the database for supporting commercially available visualization and analytical tools that allow US-CERT analysts to quickly visualize relevant relationships between disparate data and indicators of interest by presenting drill-down views of data with patterns, trends, series, and associations to analyze seemingly unrelated data. These unique capabilities allow US-CERT to identify, respond, and report suspicious and/or malicious events in a more efficient and effective manner.

Due to the nature of the EADB capability as a data warehouse for post-processed NCPS data, it may contain many different types of data from various sources from across the NCPS architecture. Therefore, cyber threat information contained in the EADB could include information considered to be PII; however, that data has already undergone the governance procedures and protections as identified in the EINSTEIN 1, ENSTEIN 2, and PCAP sections above.

Digital Media Analysis Environment (DMA)

US-CERT's Digital Media Analysis environment is a segregated, closed, computer network system that is used to conduct timely investigative analysis of digital devices and their storage mediums in support of US-CERT staff and constituents. Devices may include, but are not limited to, hard disk drives, USB thumb drives, and mobile phones and devices. Using leading edge technology and industry standard forensic procedures, the DMA allows US-CERT analysts to develop insight into the cause and effect of confirmed cyber intrusions and establish mitigation strategies to help reduce the impact of current and future compromises.

Media collected and analyzed through the DMA is voluntarily submitted to US-CERT by NCPS participants. Upon receipt of a request for DMA analysis and approval from the Chief, Digital Analytics Branch, analysts conduct forensic analysis using a copy of the media. In the event that PII is discovered, analysts will notify the Branch Chief and use US-CERT SOPs to remove PII from the media being analyzed. Once analysis is completed, any malware artifacts requiring further analysis in the AMAC are stored in a password protected zip file. All DMA artifacts undergoing analysis in

NCPS are protected in accordance with documented security controls and information handling SOPs.

Advanced Malware Analysis Center (AMAC)

The NCPS AMAC is a set of capabilities that provide a segregated, closed, computer network system that is used to analyze computer network vulnerabilities and threats. Typically, the AMAC receives information about computer security vulnerabilities and threats in the form of actual malicious code submitted to US-CERT. Once received, analysts use the malware analysis capabilities to analyze the code or images in order to discover how to secure or defend computer systems against the threat. The corrective action information is then published in US-CERT products such as vulnerability reports or alerts or malware reports.

In some cases, US-CERT receives reports of potential cyber threats from the public or government agencies through a web page dedicated to the AMAC (http://malware.us-cert.gov), which may be further analyzed or investigated in the AMAC. Information transmitted to US-CERT through the AMAC may include: malicious codes, computer viruses, worms, spyware, bots, and Trojan horses.[15] In general, any form of an attack tool are transmitted into this closed environment since they, and the vulnerabilities exploited when an attack occurs, would present a real and present danger if exposed to real operating systems and networks. Only information that relates to a known or suspected cyber threat is retained and everything else is deleted. The AMAC is focused on malware not PII and deletes any PII in accordance with its SOPs not related to its work or processes.

By conducting this analysis, the AMAC plays a critical role in improving the security of federal government computer systems as well as enhancing non-federal cybersecurity.

Information Sharing

The NCPS information sharing capability provides US-CERT, FNS, CICPA, and GCSM with a secure environment for sharing cybersecurity information with a wide range of security operations and information sharing centers across federal, state, local, tribal, private, and international boundaries.[16] The objective of the information sharing capability is to prevent cybersecurity incidents from occurring through improved sharing of threat information, reduce the time to respond to incidents through improved coordination and collaboration capabilities, and improve efficiencies through the use of more automated information sharing and through the exposure of analysis capabilities.

CyberScope

In 2010, the Office of Management and Budget (OMB) issued two memoranda (OMB 10-15 and OMB 10-28), instructing DHS to assume reporting responsibilities for all D/As on FISMA

[15] While the AMAC maintains a separate website for these reports of incidents, US-CERT analysts use the same processes and procedures for protecting PII that are described throughout this PIA.

[16] NSD solicits functional requirements from each of these branches to ensure the NCPS information sharing capability meets their mission needs.

requirements using a web-based tool called CyberScope.

Within DHS, the FISMA reporting responsibility falls within NPPD's NCSD, with program responsibilities managed by FNS and operational responsibility managed by NSD.

CyberScope was developed by the Department of Justice (DoJ) and has been used for FISMA reporting since 2009. Under OMB Memorandum 10-15 (April 21, 2010), OMB called for federal agencies to report their 2010 FISMA compliance through CyberScope, and assigned to DHS the responsibility to provide additional operational support to Federal agencies in securing federal systems.

OMB Memo 10-28 (July 6, 2010) further clarified that DHS will exercise primary responsibility within the executive branch for the operational aspects of federal agency cybersecurity with respect to the federal information systems that fall within FISMA under 44 U.S.C. § 3543.

Specifically, DHS is required to:

- Oversee the government-wide and agency-specific implementation of and reporting on cybersecurity policies and guidance;
- Oversee and assist government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity;
- Oversee the agencies' compliance with FISMA and developing analyses for OMB to assist in the development of the FISMA annual report;
- Oversee the agencies' cybersecurity operations and incident response and provide appropriate assistance; and
- Review, on an annual basis, the agencies' cybersecurity programs.

CyberScope is a Sensitive But Unclassified (SBU) web-based application that supports approximately 117 reporting agencies through connections with OMB's MAX Portal, which requires two-factor authentication in accordance with Homeland Security Presidential Directive (HSPD)-12.

The OMB MAX Portal[17] is part of the OMB MAX Federal Community, and is used by OMB and federal agencies to share information and collaborate. It is part of the Budget Formulation and Execution Line of Business (BFELoB).

US-CERT.gov Website and Portal

In order to provide up to the minute information about US-CERT and to carry out its mission in close collaboration with its partners and constituents (federal D/As, state, local, and tribal governments, industry, academia, the general public, and international partners) along with other branches of NCSD, US-CERT utilizes the US-CERT.gov website and portal. The US-CERT.gov website allows for the dissemination of general information to the public about US-CERT and its

[17] New users to the OMB MAX Portal can register for access via the link: https://max.omb.gov/maxportal/home.do.

activities, as well as information pertinent to the discipline of cybersecurity. Additionally, the website is the primary means for members of the public to interact with US-CERT, request information, and report incidents. There are four forms located on the website used to accomplish these objectives:

1) The Cyber Security Evaluation Tool (CSET) International Organization for Standardization (ISO) form (CSETISO) - requests the name and email address of those seeking to download the CSET in ISO image format. All requested fields are optional.

2) The Industrial Control Systems Joint Working Group (ICSJWG) form requests the name, telephone number, and email address of presenters (and, optionally, co-presenters) at an upcoming ICSJWG meeting. Contact information for the presenter must be provided in order to submit the form.

3) The Mail lists form requests the email address of subscribers to the National Cyber Awareness System (NCAS) mailing lists. The email address must be provided in order to subscribe or unsubscribe. It is possible for the submitted email address format to include a name, which may be present but which is not required.

4) The Report form requests the name, email address, and telephone number of those using the US-CERT Incident Reporting system to report an incident. Contact information for the reporter must be provided in order to submit the form.

Data submitted via the Report form is fed directly to the IMS ticket tracking system as described earlier in the PIA. PII data submitted via the other forms reside on secured web servers within the US-CERT.gov environment and are retained for the sole purposes of disseminating information to form submitters using an automated script, and to periodically provide US-CERT with aggregate statistical figures regarding dissemination of information.

The US-CERT.gov portal allows for interactions among US-CERT analysts and its stakeholders to provide reasoned, credible, and actionable cyber security information. The US-CERT.gov portal also provides a secure, web-based collaborative system to share sensitive cyber related information with its partners and constituents, including the interactions with the Government Forum of Incident Response and Security Teams (GFIRST).[18] US-CERT maintains SOPs that prohibit the sharing and storage of PII on the US-CERT.gov portal, and content is periodically reviewed by US-CERT analysts to ensure that no PII resides in the portal.

[18] GFIRST is a group of technical and tactical practitioners from incident response and security response teams responsible for securing government information technology systems and providing private sector support in the U.S.

Cyber Indicators Repository (CIR)/Cyber Indicators Analysis Platform (CIAP)

The NCPS CIR and CIAP is the first capability release of the NCPS information sharing capability. The CIR and CIAP systems are designed to be a common repository for sightings[19] and indicators. The CIAP contains data restricted for access and use by authorized US-CERT analysts only. The CIR contains data for access and use by authorized federal .gov and .mil users through the GFIRST compartment of the US-CERT.gov portal. The CIR and CIAP are collaborative tools that allow authorized, trained, and trusted users to add, edit, and remove data as appropriate. Users may add sightings to the database and associate indicators (IP addresses, domains, email headers, files and strings) with the sightings. Users may also search on cyber threat data added by other users.

These systems allow US-CERT and its federal constituents the ability to mutually deliver operationally relevant data in an efficient and effective manner, providing a 24/7 operational service that the Computer Network Defense (CND)[20] community critically needs. The systems provide US-CERT and its mission partners with the capability to collect, correlate and exchange up-to-date threat data during its daily operations.

The information contained in CIAP comes from a variety of sources, including the following: analysis by US-CERT; data submitted to US-CERT from government D/As, military branches, and possibly commercial companies; and reports received from vendors and industry partners that are deemed useful to US-CERT research. Both systems contain cyber indicators - human-readable cyber data used to identify some form of known or suspected cyber threats - and data related to: IP addresses and domains (associated information, such as the associated port, publicly available WHOIS[21] information, and Uniform Resource Identifiers (URI)); email headers (message attributes such as the sent date, subject, links, attachments, sender's name and sender's e-mail address); and files (malware and associated information including the file's size, hash values, and behavior). In addition, CIAP contains strings (persistent and unique identifiers specific to malicious activity). Each of these categories has multiple, specific features or characteristics, which may be captured from, and assigned to an indicator, depending on the circumstances for which the indicator is being captured. The user information includes the user's first name, last name, user ID, agency, phone number, and email address. The user information is collected in order to associate inputted entries

[19] Sightings are defined as a set of indicators that have been seen or reported at a given time.

[20] The computer network defense (CND) community is comprised of analysts from US-CERT's constituent organization who are conducting network defense operations as part of their daily duties.

[21] WHOIS is a Transmission Control Protocol (TCP)-based transaction-oriented query and response protocol that is commercially available and 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. (http://www.ietf.org/rfc/rfc3912.txt). DHS subscribes to and receives commercially and publicly available WHOIS information which includes: person and organization names, addresses, emails, phone numbers, contact information (address, email, and phone) for both administrative contacts as well as technical contacts. The Internet Corporation for Assigned Names and Numbers (ICANN) is the keeper of the WHOIS database and each of the domain providers who register domains with ICANN WHOIS service must be informed that the data is public, and users have no reasonable expectation of privacy.

with a user for auditing purposes and to provide a contact should a user want to inquire about database data from the user who inputted the data. Only PII that is associated with information about a known or suspected cyber threat should be input into the database and users are skilled and trained in identifying what data to enter. Also, all CIR users agree to abide by specific rules of behavior and responsibilities with regard to access and to the quality of data that is permitted to be uploaded.

Once the NCPS information sharing capability is fully deployed, it will help facilitate the exchange of information on cybersecurity among US-CERT, FNS, CICPA, GCSM, D/As, state, local, and tribal governments, private organizations, foreign Computer Security Incident Response Teams (CSIRTs), and the public.

Intrusion Prevention

EINSTEIN 3 Accelerated (E^{3}A)

Finally, the NCPS will include an intrusion prevention capability (operationally known as E^{3}A). EINSTEIN 1 and 2 allow DHS to analyze federal executive branch traffic, as approved by the relevant authorities, and to detect malicious traffic. With E^{3}A, DHS will not only be able to detect malicious traffic, but also prevent it. This will be accomplished by delivering intrusion prevention capabilities as a Managed Security Service (MSS)[22] that will be provided by Internet Service Providers (ISPs) for intrusion prevention and threat-based decision making on network traffic entering or leaving the federal executive branch networks.

When a signature alerts on known or suspected cyber threats, E^{3}A will act on that threat to prevent harm to the intended targets. Intrusion prevention will improve NCSD's ability to keep federal civilian networks secure.

DHS will develop its own signatures and responses to known and suspected cyber threats, and adapt those made available by US-CERT mission partners. Information sharing on cyber threats with mission partners will be conducted in accordance with all applicable laws and oversight policies and procedures including DHS's privacy requirements.

This PIA discusses the privacy impacts, risks, and mitigations for the NCPS suite of capabilities as outlined in the overview above; the information that resides on it and is collected, transmitted, and analyzed within it. NPPD has identified four general categories or types of information collected within the NCPS:

1) Information collected from and about individuals who submit cyber threat incident report information to US-CERT via telephone, fax, or the Internet;
2) Contact information collected from individuals to provide subscription or registration services offered through the US-CERT.gov website and the US-CERT.gov portal;

[22] MSS is a model by which the government articulates the objectives and services levels expected for their constituencies. MSS providers then determine how, where, when, and at what cost, those services will be delivered.

3) General contact and other related information used to grant access to employees, contractors, and other individuals to the US-CERT.gov portal, and compartments within the US-CERT.gov portal; and

4) Information regarding known or suspected cyber threats collected from federal D/As, state, local, and tribal governments, industry, the general public, and international partners.

Information collected in the first three categories is covered under existing DHS Department-wide PIAs and System of Records Notice(s) (SORN(s)) maintained by DHS and will be generally discussed in the analysis section of this PIA. The analysis section of this PIA will primarily discuss the fourth category – information regarding known or suspected cyber threats and any collection, use, storage and disposal of information that could be considered PII as part of that collection.

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 provide the justification for US-CERT practices that are enabled by the network and sensors:

1) *Federal Information Security Management Act* (44 U.S.C § 3546) establishes that there will be a federal information incident security center. That center is US-CERT.

2) *Homeland Security Act of 2002 (*6 U.S.C §§ 121 and 143) 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 CI/KR of the United States and recommended measures necessary of protection.

3) *HSPD 7: Critical Infrastructure Identification, Prioritization, and Protection,* December 17, 2003; require US-CERT to aid in national recovery efforts for CI/KR.

4) *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 NCSD: Securing Governments' Cyberspace, a National Cyberspace Security Awareness (and training) Program, and a National Cyberspace Security Response System.

5) *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.

6) *NSPD-54/HSPD 23*: Comprehensive National Cybersecurity Initiative, January 8, 2008.

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

8) *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).

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

The Department of Homeland Security system of records titled, Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (November 25, 2008) covers the following collections:

- Information collected from and about individuals who submit cyber threat incident report information to US-CERT via telephone, fax, or the Internet; and
- Contact information collected from individuals to provide subscription or registration services offered through the US-CERT portal.

The Department of Homeland Security system of records titled, Department of Homeland Security (DHS) General Information Technology Access Account Records Systems (GITAARS) September 29, 2009, 74 Fed. Reg. 49882 (September 29, 2009) covers the following collection:

- General contact and other related information used to grant access to employees, contractors and other individuals to the US-CERT portal, and compartments within the portal.

Information regarding known or suspected cyber threats collected from federal departments and agencies, state, local, and tribal governments, industry, the general public, and international partner collected through the EINSTEIN sensors, is not based on data that identifies an individual but on the security event that triggered the alert. In the rare cases when EINSTEIN 2 collects information that could be considered PII, this information will be maintained and indexed by the security incident, not by the PII. US-CERT 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. US-CERT does not retrieve this information by a personal identifier therefore a SORN is not required for this collection.

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

The NCPS includes multiple capabilities, which are performed by a number of different systems. All systems that process federal data have received a FISMA identification number and follow the DHS certification and accreditation requirements, which includes development of a system security plan. DHS system accreditations are generally valid for three years from the date of authorization. The core components of the NCPS (MOE and EINSTEIN), received their current security authorizations in July 2010.

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

NCSD 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.

NPPD has received generic clearance for the Collection of Qualitative Feedback on Agency Service Deliver for the US-CERT portal Web User Feedback forms. The OMB Control Number for this collection is: 1601-0014.

Section 2.0 Characterization of the Information

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

US-CERT may collect name, phone number, email address, and affiliation (e.g., company or agency name) from individuals both domestic and international who submit cyber threat incident report information to US-CERT via telephone, fax, or the Internet. Only name and email address are collected from individuals to provide subscription or registration services offered through the US-CERT portal.

General contact information such as name, title, company name or agency, email address, phone numbers and other business related information may be collected to grant access to employees, contractors and other individuals to the US-CERT portal, and compartments within the portal.

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 within the NCPS may consist of packets, files, system logs, and flow records, all of which could include information that could be considered PII. For example, EINSTEIN 2 monitors communications sent to the federal networks by the public and those communications generated by users of the federal networks. The information collected takes the "form" of network flow records and network packets collected in response to alerts triggered by pre-determined intrusion detection signatures. US-CERT may collect data from WHOIS, a publicly available source to associate with known threats. By assigning this data to a known threat, US-CERT may identify commonalities and patterns among threats based on their originating information. The data is not used to identify specific individuals, nor are records searchable by information that could be considered PII.

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. This additional data could include IP addresses, ports, protocols, digital signatures, time stamps, direction/type of traffic, flags, sensor name, etc.

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

For incident reporting and subscriptions for US-CERT products, sources of information include individuals, private sector entities, and personnel working at other federal or state agencies. In addition, information is also received from international sources,[23] including individuals, companies and other nation's governments. As a practical matter, sources principally include federal government network security managers and those in the private sector who are interested and willing to contribute to the catalog of incidents or analysis of the incident, primarily, those working within the CND community.

Other sources include the sensors themselves, located at various federal agency network collection points. Such information includes flow records, which identify the 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. The sensors push data to the data store on a consistent basis and do not require analyst intervention.

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

US-CERT analysts do not use commercial sources for the purpose of identifying individuals. US-CERT analysts use information from a range of sources, including commercial sources and publicly available data to verify information on cybersecurity threats (e.g., anything that could be found through open source Internet searches, newspaper articles.). This data is used to help resolve incidents that are reported to US-CERT and for historical reference of similar incidents.

[23] As noted above, the exchange of information on cybersecurity occurs between DHS, departments and agencies, intelligence agencies, state, local, tribal governments, private organizations, foreign CSIRTs, and the public. This sharing is done in accordance with MOAs or other types of information sharing agreements, as applicable.

2.4 Discuss how accuracy of the data is ensured.

Where individuals voluntarily provide their name, email, phone number, and incident data, US-CERT may call or email the individuals to verify their information, security data, or to follow-up on a reported cyber incident submitted by the individual or organization. Individuals subscribing to US-CERT products have an interest in receiving the product information and individuals submitting an incident or malicious code information are often willing to provide further information in order to better support the information security community.

In order to assess the veracity of an incident that is reported to US-CERT, the analysts:

1) Capture incident data;
2) Verify the data through closed or open source research, e.g., Google, EINSTEIN flow data;
3) Contact the system owner;
4) Triage the incident, identify other affected parties and contact them; and
5) Work with the affected party or organization to identify mitigation strategy.

However, with regard to sensor or other capability derived source, the hardware maintains exact copies of intrusion detection information transmitted to or from the federal network. For example, if a connection "spoofs" an IP address (manipulates the data packets it transmits to the federal network to appear as if being sent from one source when in fact they come from another source) the intrusion detection system will simply record those packets with the "spoofed" IP address. The system only keeps a copy of the spoofed IP address; therefore data collected by a sensor is accurate because it is an exact copy of the data available.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: NCPS may collect more data than is necessary and due to the nature of how the data is collected, some information may be inaccurate or fraudulent.

Mitigation: For contact information collected from individuals to provide incident reports, request subscription or registration services offered through the US-CERT portal or general contact and other related information used to grant access to employees, contractors, and other individuals to the US-CERT portal, and compartments within the portal, US-CERT collects the minimum information necessary directly from the individuals.

As a general rule, the NCPS only collects data that is necessary to accomplish its mission. For information collected from the person reporting the incident, analysts may attempt to confirm the integrity of the data received through the voluntary submissions by contacting the individual through phone or email. When provided, this includes the contact information of the person reporting the incident (if applicable), incident data, which may include IP and host addresses and flow data, and actions taken to resolve the incident.

Any information that is collected must be considered to be directly relevant and necessary to accomplish the specific purposes of the program; if it is not, the US-CERT analyst is trained to notify the US-CERT Oversight and Compliance Officer and to delete it in accordance with US-CERT SOPs.

When sensors are involved, the malicious activity is captured along with the data predetermined to be analytically relevant to that threat. Captured data is only accessed by the intrusion detection computer program. When data is captured due to an alert being triggered, there is a slight risk that information that could be considered PII may be transmitted along with a malicious activity. This risk is initially mitigated by establishing specific rule-based signatures developed to identify specific malicious activity.

The privacy risk is also mitigated by limiting how the intrusion detection information is viewed, as the captured data is only accessed by the intrusion detection computer program. The only detailed computer network traffic data that analysts see is the limited portions of the traffic that is specifically tailored to support an alert of an instance of known malicious activity as defined by a signature, and in those limited situations, only trained US-CERT analysts view the traffic data. If network traffic does not meet the specific criteria for a specific signature, that network traffic is not viewed by US-CERT. In addition, the sensors are designed to maintain the integrity of the information to ensure that unauthorized modifications cannot be made. Finally, US-CERT follows SOPs, which require a review of collected information that could be considered PII and only that information that is analytically relevant is retained, all other information is deleted.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Using network flow records, US-CERT can detect certain types of malicious activity and coordinate with the appropriate federal executive agencies to mitigate those threats and vulnerabilities.

Certain sensors alert US-CERT analysts when specific malicious network activity is detected, and provide US-CERT with increased insight into the nature of that activity. These sensors use a set of custom signatures based upon known or suspected cyber threats. Signatures are technical descriptions of known or suspected cyber threats to 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. Signatures are derived from numerous sources such as commercial or public computer security information; incident reports to US-CERT; information from federal partners; or in-depth analysis by US-CERT.

For illustrative purposes only, the following is an example of a commercially available signature. (This is not a signature US-CERT intends to use.)

```
alert tcp any any -> $HOME_NET 443 (msg:"DoS Attempt";
flow:to_server,established; content:"|16 03 00|"; offset:0; depth:3; content:"|01|";
within:1; distance:2; byte_jump:1,37,relative,align; byte_test:2,>,255,0,relative;
reference:cve; classtype:attempted-dos; sid:2000016; rev:5;)
```

Signatures target known or suspected cyber threats by identifying specific characteristics of those threats. Some of those characteristics could be information that could be considered PII. For example, if a cyber threat chooses to use a particular email address as a "return email address," a signature could use that same "return email address" as a characteristic of that particular threat. This does not mean the "return email address" is associated with an actual person. It also does not mean that US-CERT would consider that "return email address" as an actual email address to communicate with an actual person. In this example, the "return email address" would only be used as a characteristic of that particular cyber threat. Accordingly, while the sensor will collect some information that could be considered PII, the purpose for collecting this information is to accurately identify known or suspected cyber threats by searching for a collection of characteristics for each threat.

NCSD has a governance structure for the creation and review of signatures and a process by which the NCPS alerts US-CERT of a known or suspected cyber threat. The signature development process determines whether particular signatures will direct the capture of associated traffic and how much traffic must be collected based on the particular cyber threat in accordance with US-CERT written procedures and subject to review by the Office of General Counsel, the US-CERT Oversight and Compliance Officer, as well as the DHS and NPPD Privacy Offices. US-CERT will deploy signatures that use PII only if the signatures have been approved in accordance with written procedures and only for the purpose of detecting cyber threats. If a deployed signature identifies more agency traffic than is necessary or relevant to understand cyber threats, or detects false positives, that signature will be reviewed and modified or removed, thus further limiting the amount of data US-CERT analysts receive.

As information or data are received by US-CERT analysts, the data is screened to determine whether it includes any PII. If PII is identified, the analyst determines whether it is pertinent to the incident under review. If it is not, the analyst deletes the PII.[24]

If the US-CERT analyst determines that the PII is relevant, it is marked accordingly and both the immediate supervisor and the US-CERT Oversight and Compliance Officer are notified and verification sought. If there is agreement that it must be retained, the proposed retention policy discussed in Section 5.1 is followed. The information is encrypted and access to the file is restricted

[24] Residual traces of PII are not wiped clean from potential storage devices. US-CERT follows Standard Operating Procedures (SOP) in which the analyst will overwrite, redact, or replace PII data that is not necessary to understand the analysis or product.

to authorized users only. When the incident is entered into the incident handling system, a notation is made that indicates whether or not the incident involves PII. However, no PII is included in the ticketing records. If PII is maintained as part of the record and needs to be disseminated, written approval must be obtained in advance of dissemination from the US-CERT Director.

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.

While the EADB function of the NCPS includes query capabilities, no applications that constitute the NCPS are configured or used to complete queries based on PII. Queries are limited to data and indicator information necessary to identify trends and patterns in cyber threat indicators and disparate data sets.

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

Only US-CERT analysts and MOE administrators have access to the components of the NCPS system used for analysis and reporting. In addition, access to EINSTEIN data collected through the DHS Trusted Internet Connection (TIC) EINSTEIN sensors can be accessed by the Customs and Border Protection (CBP) security operations center (SOC).[25] Other components with assigned roles include D/As, CIKRs, commercial CERTs and international partners with authorization to access the products and information disseminated by US-CERT through CIR.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that information that could be considered PII could be used for purposes other than to identify specific known or suspected cyber threats.

Mitigation: US-CERT analysts as well as NCPS administrators and information assurance personnel are trained on both DHS and US-CERT specific procedures for handling and safeguarding PII. Analysts, administrators and information assurance personnel receive training upon hire, and are required to take refresher training each year on Security Education and Awareness Training (SEAT). In addition, US-CERT maintains 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 for specifically identified roles and responsibilities.

In addition, access to the NCPS is restricted to individuals with demonstrated need for access,

[25] The DHS Security Operations Center (SOC) is managed by the DHS Customs and Border Patrol (CBP) Component. In order to comply with Department level FISMA reporting metrics, all DHS Components are required to report any incidents related to DHS networks to the CBP SOC on a weekly basis. As a result, if there is a confirmed incident on a NCPS system, details of the incident will be reported to CBP through their DHS Enterprise Operations Center (EOC) Portal application.

and such access must be approved by the supervisor as well as the NCSD Information System Security Managed (ISSM)/Security Manager. Users must sign Rules of Behavior which identify the need to protect PII prior to gaining access. Access to the NCPS MOE is only available via two factor authentication. Once the user is logged in to the MOE, certain applications that reside on the MOE require single-factor authentication in order to be granted 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.

Privacy Risk: There is a risk that information that could be considered PII would be retained for longer than necessary.

Mitigation: During packet collection, all packets older than 30 days that are not determined to be analytically relevant to a cyber threat are purged.[26]

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.

This PIA serves as notice of the NPPD NCPS program. Notice is also provided through previously published DHS cybersecurity-related PIAs.

If an individual reports an incident by telephone, their contact information is not required to report a cyber-related incident. When submitting an incident via email or through US-CERT website, contact information is required. In those circumstances, notice is provided to the reporting individual regarding the potential uses of the information of the individual prior to their submission of the incident. Further notice is provided by the Privacy Policy available at the following site http://www.us-cert.gov/privacy.html#privacy.

This collection of personal information is covered by the Department of Homeland Security system of records titled, Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (November 25, 2008) and The Department of Homeland Security system of records titled, Department of Homeland Security (DHS) General Information Technology Access Account Records Systems (GITAARS) 74 Fed. Reg. 49882 (September 29, 2009) covers the following collection.

Users of federal computer systems are provided with logon banners and sign user agreements that specifically notify them of the computer network monitoring. This Privacy Impact Assessment also serves as a general notice to individuals that network traffic flowing to or from participating federal executive agencies may be collected for computer security purposes.

[26] See Section 5.0 for discussion on retention schedule.

Furthermore, with regard to the information collected from the sensors, federal agencies are required to post notices on their websites as well as at other major points of entry that computer security information is being collected and their system monitored. Such notices cover intrusion detection systems like EINSTEIN 2.

Participating agencies using the sensors are required to certify to US-CERT that they have appropriate notices, banners, or measures in place to provide individuals with notice that their interaction with federal networks is subject to monitoring for computer network security purposes.

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

For incidents reported to US-CERT, individuals have the right to voluntarily provide (or decline to provide) their contact information when submitting information regarding a cyber-related incident or submitting a trouble ticket. If the submitter chooses to not provide such information, US-CERT will still process the report based on what information has been provided.

PII may be required in order to process or respond to queries made by individuals to the federal government, but it is not mandatory that an individual produce this information. Individuals that subscribe to receive US-CERT products may opt-out of this service at any time by contacting US-CERT.

In addition, all individuals (employees and contractors) 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. These users can then decide if they wish to use the system or not, and decide what information they want to transmit over the government system.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals reporting a cyber incident to US-CERT may not realize their PII is being retained or that an individual may choose not to read the notice or banner provided or be aware of the information collection occurring under the NCPS program.

Mitigation: For individuals reporting a cyber incident to US-CERT, a statement is included during the reporting process for the IMS to ensure that the individual has adequate notice of the collection and the potential uses of the information. For example, if a report is taken through the phone, the call agent is required to give notice to the person that any information they provide is voluntary, and if they choose to provide information, their information will be used for limited purposes. Contact information is collected, although not required, in order for the researcher assigned to the code or incident to follow up with the original submitter should the information available be incomplete or inaccurate

In the course of normal operations, it is possible that information that could be considered PII could be collected through the submission of suspicious code, spam, or malware. In the event this information is collected, US-CERT analysts are required to follow SOPs for the handling of this information. As part of the SOP the information will be reviewed by the US-CERT Oversight and Compliance Officer and the NPPD Office of Privacy. If data-owner notification is appropriate, it will be directed by the US-CERT Oversight and Compliance Officer.

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.

According to US-CERT SOPs analysts must review each file to be retained to determine whether it contains information that could be considered PII. US-CERT will only retain PII if it is specifically determined to be analytically relevant to a particular cyber threat. All other information that could be considered PII can be discarded when determined false or non-malicious. In these cases, all information is subject to periodic retention reviews.

However, until the records in the system have a NARA-approved disposition schedule, the records must be considered permanent and are retained indefinitely via encrypted tapes.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that PII could be maintained unnecessarily.

Mitigation: There may be incidents reported or packets received that include PII. The analysts are required to review all data collected to determine whether PII exists and whether it is analytically relevant to a particular cyber threat. If the US-CERT analyst determines that the PII is relevant, it is marked accordingly and both the immediate supervisor and the US-CERT Oversight and Compliance Officer are notified and verification sought. The information is encrypted and access to the file is restricted to authorized users only. While the incident is entered into the incident handling system, a notation is made that it includes PII. No PII is included in the ticketing records. If PII needs to be disseminated, written approval must be obtained in advance of dissemination, from the US-CERT Director.

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.

Yes. Federally-recognized cyber centers, civilian agencies such as the security operations centers for the respective department or agency, state, local, tribal government, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order may have access to US-CERT's technical products. Sharing of information with international data sharing partners is done in accordance with Memoranda of Agreements (MOAs) or other types of information sharing agreements, as applicable. However, only US-CERT authorized users can see the personal contact information gathered through the IMS or through US-CERT.gov, and unless the data owner authorizes the sharing of their information, it is not provided to anyone outside of DHS.

As part of its computer network security responsibilities, US-CERT generates reports on topics including general computer network security trends; specific incidents; and, anomalous or suspicious activity observed on federal networks. The identification of the specific individual or entity that established the network connection that triggered an alert is not included in the reports. These reports are made available to DHS organizations, including the National Cybersecurity and Communications Integration Center (NCCIC), and other federal executive agencies through systems such as the US-CERT.gov secure website for their use in infrastructure protection and other computer network security related responsibilities. Computer network security is, however, accomplished using multiple disciplines to secure the federal network and part of this support is provided by law enforcement, intelligence, and other agencies. These other agencies are notified when a computer network event occurs that falls under their responsibility.

In accordance with its SOPs, US-CERT also notifies law enforcement or an intelligence entity of incidents of relevance to the mission, primary jurisdiction or other applicable authorities for action.

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

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

As applicable, the routine uses for the NCPS data, are governed by the DHS system of records titled, DHS/All-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (November 25, 2008) and The Department of Homeland Security system of records titled, Department of Homeland Security (DHS) General Information Technology Access Account Records Systems (GITAARS) 74 Fed. Reg. 49882 (September 29, 2009).

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

Cyber threat information received through the EINSTEIN sensors or other means are not retrieved by a personal identifier and thus do not require a System of Records Notice.

6.3 Does the project place limitations on re-dissemination?

Cyber threat information received through the EINSTEIN sensors or other means are 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 in advance of dissemination, from the US-CERT Director in accordance with US-CERT SOPs.

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

In the event that PII must be released, it is released with the written approval of the US-CERT Director, and in compliance with the Privacy Act, as such the disclosure of a record is for the explicit use and purpose compatible with the purpose for which it was collected. The Privacy Act conditions for disclosure shall also apply, except when pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. Accounting for such disclosures are made in accordance with each system of record under its control and exceptions as described therein.

US-CERT provides cyber related information to the public, federal departments/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 which precipitated the product itself.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that PII could be shared inappropriately.

Mitigation: Unauthorized disclosure is mitigated through various means, including encrypting the information and limiting who has access to the information. US-CERT maintains specific SOPs governing the use of information, including information that could be considered PII. All information that could be considered PII is reviewed and that information is only shared if it is determined to be analytically relevant to a particular cyber threat. If a report containing PII is developed or modified for multiple audiences, each version is reviewed for appropriate markings. Handling and dissemination instructions are also included and sources and methods are redacted. Law enforcement sensitive information is not to be released without originating agency approval. Guidelines are provided within US-CERT SOPs.

Section 7.0 Redress

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

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/foia. The release of information is subject to standard FOIA exemptions.

With respect to information collected through the sensors, the information is not based on data that identifies an individual but on the security event that triggered the alert. In the rare cases when EINSTEIN 2 collects information that could identify a person (e.g., an unspoofed email address within header information or other PII within records incidentally collected as part of a security incident), this information will be maintained and indexed by the security incident, not by the PII. This means that there will not be a list of email addresses or names kept but a log of what intrusion occurred or other security event; analysts will sort the data by pulling up security events not email addresses. Also, EINSTEIN 2 retrieves information via signatures, analyses, and reports, not by PII. The security event which triggered the alert is how data is retrieved and stored. As such, there is no information about an individual that can be accessed.

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

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.

There are no separate procedures for individual correction of information collected by the sensors since flow records and alerts are generated from exact copies of computer network traffic.

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

If the submission is through the IMS, the system asks the individual to verify their information prior to the final submission of the data. If the individual contacts the Call Center and speaks to a representative, the representative verifies the individual's contact information prior to ending the telephone call. Submission of contact information is voluntary.

Individuals that subscribe to receive US-CERT products are provided notice at the time of collection that they may correct their information or opt-out of this service at any time by contacting US-CERT.

An individual can also 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.

With regard to sensor-collected information, there are no separate procedures for individual correction of information since flow records and alerts are generated from exact copies of computer network traffic. The US-CERT analyst's use of the system is recorded, and analysts are specifically trained to ensure that the use of collected data is focused solely on the malicious activity data and not on the personal content of the communications, or to obtain the personal information about the source of the malicious activity.

7.4 Privacy Impact Analysis: Related to Redress

There are no redress procedures beyond those described above and afforded under the Privacy Act and FOIA.

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?

Quarterly internal reviews are carried out by the US-CERT Oversight and Compliance Officer, along with the NPPD Senior Privacy Analyst, to evaluate and assess compliance with the information handling procedures as outlined in the US-CERT SOPs. Additionally, specific information handling SOPs to ensure awareness, accountability, and compliance of what information should and should not be shared, are circulated annually to the US-CERT analysts.

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

Access to the NCPS is restricted to individuals with a demonstrated need for access, and such access must be approved by the supervisor as well as the NCSD ISSM/Security Manager. Users must sign Rules of Behavior that identify the need to protect PII prior to gaining access. Access to the MOE is only available via two-factor authentication. All NCPS users are trained to protect privacy information. Their actions are logged, and they are aware of that condition. In addition, certain applications, including CIR, maintain Rules of Behavior for all users. 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. NPPD employees are also required to complete annual SEAT requirements. 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.

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

Users must obtain a favorable DHS suitability determination[27] prior to acquiring access to certain NCPS systems. 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 the access form (e.g., analyst, user, general user, system admin., network admin.). The NCPS access form must be completed by the government supervisor within the branch that the individual will be supporting. The user's role is defined by the branch manager and validated by the ISSM/Security Manager. Accounts are reviewed monthly by the ISSO to ensure that accounts are maintained and current. In addition, user account activity is logged, and the logs are reviewed each day. Users accessing EINSTEIN and the US-CERT portal through which NCPS disseminates information are adjudicated through their own organization.

In addition, US-CERT maintains SOPs on privacy protection for the purpose of identifying sensitive information, and for the proper handling and minimization of PII, which outlines the necessary procedures and defines the terms, for specifically identified roles and responsibilities. These SOPs are provided to all US-CERT employees during training and are circulated to US-CERT analysts so that they are aware of what information should and should not be shared with its information sharing partners.

[27] The suitability determination is a process that evaluates a 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.

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
NCPS Program Manager
National Cyber Security Division
National Protection and Programs Directorate
Department of Homeland Security
(703) 235-2853

Approval Signature

Original signed and on file with the DHS Privacy Office.

____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix – Acronym List

Advanced Malware Analysis Center (AMAC)
Budget Formulation and Execution Line of Business (BFELoB)
Commercial-Off-The-Shelf (COTS)
Computer Network Defense (CND)
Computer Security Incident Response Teams (CSIRTs)
Critical Infrastructure Cyber Protection and Awareness (CICPA)
Critical Infrastructure/Key Resources (CI/KR)
Customs and Border Protection (CBP)
Cyber Security Evaluation Tool (CSET)
Cyber Indicators Analysis Platform (CIAP)
Cyber Indicators Repository (CIR)
Department of Homeland Security (DHS)
Department of Justice (DoJ)
Departments and Agencies (D/A)
Destination Internet Protocol (DIP)
Development & Test (Dev/Test)
Digital Media Analysis Environment (Forensics)
Domain Name System (DNS)
EINSTEIN 3 Accelerated (E^3A)
Enhanced Analytical Database (EADB)
Enterprise Operations Center (EOC)
Federal Information Security Management Act (FISMA)
Federal Network Security (FNS)
Freedom of Information Act (FOIA)
General Information Technology Access Account Records Systems (GITAARS)
Global Cyber Security Management (GCSM)
Government Forum of Incident Response and Security Teams (GFIRST)
Homeland Security Presidential Directive (HSPD)
Incident Management System (IMS)
Industrial Control Systems Joint Working Group (ICSJWG)
Incident Management System (IMS)
Internet Corporation for Assigned Names and Numbers (ICANN)
Information Sharing and Analysis Centers (ISACs)
Information System Security Manager (ISSM)
Information System Security Officer (ISSO)
Information Technology (IT)
Input/Output (I/O)
International Organization for Standardization (ISO)
Internet Protocol (IP)
Internet Service Provider (ISP)

Intrusion detection system (IDS)
Managed Security Service (MSS)
Massively Parallel Processing (MPP)
Memoranda of Agreements (MOAs)
Mission Operating Environment (MOE)
National Archives and Records Administration (NARA)
National Cyber Awareness System (NCAS)
National Cyber Security Division (NCSD)
National Cybersecurity and Communications Integration Center (NCCIC)
National Cybersecurity Protection System (NCPS)
National Protection and Programs Directorate (NPPD)
Network Security Deployment (NSD)
Office of Management and Budget (OMB)
Packet Capture (PCAP)
Paperwork Reduction Act (PRA)
Passive Domain Name System (pDNS)
Personally Identifiable Information (PII)
Privacy Act (PA)
Privacy Impact Assessment (PIA)
Security Education and Awareness Training (SEAT)
Security Information and Event Management (SIEM)
Security Operations Center (SOC)
Sensitive But Unclassified (SBU)
Source Internet Protocol (SIP)
Standard Operating Procedures (SOP)
Storage Area Network (SAN)
System of Records Notice (SORN)
Transmission Control Protocol (TCP)
Trusted Internet Connections (TIC)
Uniform Resource Identifier (URI)
United States–Computer Emergency Readiness Team (US-CERT)
Yet Another Flowmeter (YAF)