Privacy Impact Assessment
for the
Initiative Three Exercise

March 18, 2010

Contact Point
United States Computer Emergency Readiness Team (US-CERT)
(888) 282-0870

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

Pursuant to Initiative Three of the Comprehensive National Cybersecurity Initiative, DHS is engaging in an exercise to demonstrate a suite of technologies that could be included in the next generation of the Department's EINSTEIN network security program. This demonstration, (commonly referred to as the "Initiative Three Exercise" or, more simply, as "the Exercise") will use a modified complement of system components currently providing the EINSTEIN 1 and EINSTEIN 2 capabilities, as well as a DHS test deployment of technology developed by the National Security Agency (NSA) that includes an intrusion prevention capability (collectively referred to as "the Exercise technology"). The purpose of the Exercise is to demonstrate the ability of an existing Internet Service Provider that is a designated as a Trusted Internet Connection Access Provider (TICAP) to select and redirect Internet traffic from a single participating government agency through the Exercise technology, for US-CERT to apply intrusion detection and prevention measures to that traffic and for US-CERT to generate automated alerts about selected cyber threats. This PIA is being conducted because the Exercise will analyze Internet traffic which may contain personally identifiable information (PII).

Reason for the PIA

Certain aspects of the Exercise are classified. The DHS Privacy Office conducted a full classified PIA of the Exercise and made that PIA available consistent with the classification restrictions. The DHS Privacy Office conducted this PIA in order to provide public transparency regarding the publicly releasable aspects of its assessment of the Initiative 3 Exercise.

Introduction: The Initiative Three Exercise

The Exercise will enable DHS to demonstrate additional capabilities beyond those available in the EINSTEIN 2 intrusion detection system (IDS). An IDS primarily observes and reports or issues alerts about cyber threats. The Exercise will deploy technology that will include intrusion detection and add intrusion prevention. The Intrusion Prevention System (IPS) capability to be used in the Exercise will enable DHS to respond appropriately to counter known or suspected cyber threats identified within the participating agency's network traffic carried by the TICAP.

The goal of the Exercise is to pilot EINSTEIN 3 capabilities based on technology developed by the NSA and to solidify processes for managing and protecting information gleaned from observed cyber intrusions against civilian Executive Branch systems.

Once the Exercise is completed, DHS will determine which technologies and methodologies to use in implementing the Initiative Three capabilities.

Initiative Three represents the next evolution of protection for civilian Departments and agencies of the federal executive branch. This approach, called EINSTEIN 3, will draw on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision-making on network traffic entering or leaving these executive branch networks. The goal of EINSTEIN 3 is to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response. It will have the ability to automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defense. EINSTEIN 3 will assist DHS US-CERT in defending, protecting and reducing vulnerabilities on federal executive branch networks and systems. The EINSTEIN 3 system will also support enhanced information sharing by US-CERT with federal departments and agencies by giving DHS the ability to automate alerting of detected network intrusion attempts and, when deemed necessary by DHS, to send alerts that do not contain the content of communications to the NSA so that DHS efforts may be supported by NSA exercising its lawfully authorized missions. This initiative makes substantial and long-term investments to increase national intelligence capabilities to discover critical information about foreign cyber threats and use this insight to inform EINSTEIN 3 systems in real time. DHS will be able to adapt threat signatures determined by NSA in the course of its foreign intelligence and DoD information assurance missions for use in the EINSTEIN 3 system in support of DHS's federal system security mission. Information sharing on cyber intrusions will be conducted in accordance with the laws and oversight for activities related to homeland security, intelligence, and defense in order to protect the privacy and rights of U.S. citizens and U.S. Persons.

Cyber threats are any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority. Information about cyber threats may be received from government or non-government and public or non-public sources. Categories of cyber threats may include, for example phishing, IP spoofing, botnets, denials of service, distributed denials of service, man-in-the-middle attacks, or the insertion of other types of malware.

Several alternative network locations for deploying the Exercise technology were considered including at an Internet connection point housed within the individual participating agency itself or at a designated TICAP. The choice to locate the Exercise technology at the TICAP was driven by the practical necessities of cost control, scalability, USG network coverage, and speed to implementation.

The Exercise will seek to demonstrate:

1. The ability of a TICAP to redirect agency-specific Internet traffic through the Exercise technology.
2. The ability of US-CERT, utilizing the Exercise technology, to analyze redirected agency-specific traffic to detect cyber threats, and to respond appropriately to those threats.
3. The ability of US-CERT to develop techniques for supporting future EINSTEIN capabilities.
4. The ability of US-CERT to potentially share cybersecurity-related information with appropriate organizations in real-time to coordinate the cybersecurity activities of the federal government..
5. The ability of a TICAP to deliver the traffic back to the particular participating agency in a timely and efficient fashion.

This PIA is focused solely on the Exercise; it does not apply to any future EINSTEIN capability or technology.

The entities involved in the exercise will be responsible for demonstrating the following capabilities:

The participating agency will:

1. Supply the list of IP Addresses which will define and bound the traffic to be analyzed during the Exercise.
2. Certify that it has implemented procedures to ensure that network users are aware that their use of government-owned information systems is subject to monitoring and that their communications transiting through or stored on such systems may be monitored. The participating agency may use computer user agreements, log-on banners, and computer training programs to inform government users about the terms of their usage of government information systems.
3. Enter into agreements with DHS and the TICAP regarding Exercise operations.

The TICAP will:

1. Identify traffic on its network destined to or coming from the participating agency, based on a list of IP Addresses supplied by the participating agency.
2. Verify the traffic is in fact only the participating agency's traffic.
3. Redirect only the participating agency's traffic to a secured facility within the TICAP's facility where the DHS owned and operated equipment will be housed.
4. Send redirected agency traffic through the Exercise technology.
5. Send redirected agency traffic back to the TICAP's network.
6. Direct the participating agency's traffic back on its original path to or from the participating agency's network once it has passed through the Exercise technology.

7. Provide system administration services for all Exercise equipment under DHS authority.
8. Sign agreements with DHS and the participating agency regarding Exercise operations.

US-CERT will:

(Some of the specific responsibilities listed here for US-CERT will actually be performed by the Network Security Deployment Division (NSD). The NSD is another branch within the National Cyber Security Division of DHS's Office of Cybersecurity & Communications (CS&C) and is responsible, in part, for providing and managing the equipment that supports US-CERT's operations during the Exercise. For clarity and consistency with related PIAs, this PIA references US-CERT as the primary responsible DHS entity.)

1. Operate the equipment that will receive the redirected agency traffic from the TICAP.
2. Implement the signatures and scenarios to ensure collection, retention, and dissemination of only those portions of the participating agency's traffic associated with known or suspected cyber threats.
3. Monitor the mirrored traffic using classified or unclassified signatures that will be approved according to US-CERT's written procedures.
4. Generate alerts and potentially store, analyze, and retain portions of the traffic associated with known or suspected cyber threats, based on the signatures.
5. Analyze alerts and related agency traffic based on existing policies and procedures.
6. Generate automated alerts of known or suspected cyber threats based upon pre-defined criteria related to signature.
7. Respond to detected known or suspected cyber threats in the participating agency's traffic using US-CERT pre-approved methods.
8. Manage a select group of government security-cleared contractors (including those of the TICAP) to provide onsite hardware and software support for the equipment and the physical environment, under the direct supervision of US-CERT.
9. Sign agreements with participating entities regarding Exercise operation.
10. Operate all phases of the Exercise according to a set of approved standard operating procedures.
11. Provide oversight of the operation of the Exercise technology and the activities of the DHS personnel through the Oversight & Compliance Officers within US-CERT and the DHS Office of Cybersecurity & Communications.

This Exercise is designed to be executed in four distinct, consecutive phases, each built upon the capabilities demonstrated in the previous phase. The phased approach will allow the opportunity to ensure that system functionality is fully tested and validated at each phase, before proceeding to the next phase.

- **Phase One** will demonstrate the TICAP's ability to successfully redirect the participating agency's traffic. The TICAP will demonstrate that it can accurately identify the participating agency's traffic, re-direct only this network traffic to a secured facility within the TICAP's facility, and then re-insert this same traffic back from the secured facility onto the TICAP's network.
- **Phase Two** will involve the installation of the Exercise technology in the secured facility within the TICAP's facility. Planned for 30 days from completion of Phase One.
- **Phase Three** will require the TICAP to connect the Exercise technology and begin the operational portion of the Exercise during which US-CERT will begin applying the Exercise's capabilities on the participating agency's traffic against known or suspected cyber threats. The TICAP will provide system maintenance as contracted by DHS. Planned for 60 days from completion of Phase Two.
- **Phase Four**, if elected by DHS, will continue the Exercise for 12 months from completion of Phase Three. DHS's determination to extend the Exercise will include a review of various factors including: achievement of Exercise objectives and funding.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

The System and the Information Collected and Stored within the System

Describe how this update affects the amount and type of personally identifiable information collected by the program or system, and how the update compliments the previously articulated purpose of the program.

The Exercise involves a much narrower range of network traffic than the current deployment of EINSTEIN 2. EINSTEIN 2 is scheduled to deploy across all federal executive branch agencies. The only information collected, used, disseminated, or maintained during the Exercise will be limited to the Internet traffic of a single participating agency as defined by the

list of IP Addresses supplied by the participating agency and verified by US-CERT and the TICAP.

The Exercise technology will physically receive all redirected agency traffic and will apply predefined signatures to that traffic to identify known or suspected cyber threats. Only that limited portion of the redirected traffic that is associated with identified cyber threats will be available to US-CERT analysts for review. Any traffic that is not associated with a cyber threat will not be retained by US-CERT.

The additional capabilities being tested during the Exercise (IPS, classified signatures, and automated alerts) do not involve the collection or analysis of additional categories of information beyond those currently collected by EINSTEIN 2.

Signatures are based upon indicators of known or suspected cyber threats. Signatures are specific 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. Signatures may contain instructions to copy pre-defined portions of the participating agency's traffic associated with such cyber threats. Alerts from signatures contain descriptive information about the cyber threats identified by the signature. The signature development process will determine 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 Oversight & Compliance Offices of US-CERT and CS&C as well as the DHS Privacy Office and DHS Office for Civil Rights and Civil Liberties.

The automated alerts generated during the Exercise will announce the detection of known or suspected cyber threats. These notifications are generated by scenarios programmed into the Exercise technology. A scenario is a computer instruction that monitors signatures and automatically directs that certain actions, such as the generation of alerts, be taken by the Exercise technology.

During the exercise, the generated automated alerts will be similar to network flow records – they will only contain metadata about the cyber threat and will not contain the content of any network traffic beyond the inclusion of packet based metadata.

All traffic handled by the TICAP that is associated with the supplied IP addresses for the participating agency will be redirected to the Exercise technology. In the traffic there will be information that could be considered PII. US-CERT will analyze the data collected by alerts in accordance with its written information handling procedures. These procedures include methods to identify information that could be considered PII, verify whether the information specifically links to an individual, and purge that information from the analysis unless it is necessary for further US-CERT analysis.

According to the written information handling procedures, US-CERT personnel must determine that PII is necessary for subsequent US-CERT analysis in furtherance of its network security activities and protection of federal systems before such data is further processed or retained. Information deemed unnecessary for subsequent US-CERT analysis will be purged. When PII is used, US-CERT's information handling procedures require that US-CERT personnel summarize and document why the information is reasonably necessary, including a description of the cyber threat, the information in question, and why further analysis of the information is necessary. The US-CERT Director and Deputy Director will be provided with a weekly summary of instances where PII is deemed necessary for US-CERT analysis. This process is subject to review by the Oversight and Compliance Offices of US-CERT and CS&C.

Signatures are deployed in response to specific cyber threats. Should a particular cyber threat include the use of information that could be considered PII, US-CERT may deploy a signature that uses that potential PII to generate an alert. US-CERT will deploy such signatures only after the signatures have been approved in accordance with its written procedures and only for the purpose of detecting cyber threats.

If a deployed signature identifies more agency traffic than is needed to understand cyber threats, that signature will be reviewed and modified or removed, thus further limiting the amount of data US-CERT analysts receive.

US-CERT will not deploy signatures that are intended solely to identify or collect PII. The signature review process will ensure that any signature deployed and any associated data is necessary to detect, analyze, and respond to a known or suspected cyber threat.

During the Exercise, US-CERT may receive signatures, and scenarios from other agencies or organizations. A signature may contains instructions to look for particular indicators of cyber threats. Those indicators may contain information to be matched in order to find cyber threats (see example in the below Appendix from the EINSTEIN 2 PIA).

In order to prevent the participating agency from disclosing to DHS information the participating agency is prohibited from sharing, the participating agency agreed, in an MOA with DHS, to identify any particular categories of data that have special handling or security requirements. The participating agency has not identified any categories of information that require special handling or otherwise cannot be shared with DHS in connection with DHS network security activities.

In order to verify the accuracy of the traffic data used during the Exercise, US-CERT will only analyze information redirected to the Exercise technology by the TICAP. The participating agency will be responsible for accurately identifying those IP Addresses associated with its own network. The TICAP will be responsible for verifying that it is redirecting only that traffic associated with the IP Addresses the participating agency supplies.

US-CERT will perform multiple verifications of the list of the participating agency's IP Addresses based on its independent records:

- Prior to the agency traffic being redirected to DHS owned and operated equipment;
- After the first 30 days of the exercise operation; and
- At the end of the 60 day period of operation to ensure only the participating agency's traffic was redirected.

If, during the Exercise, any party determines that IP Addresses not associated with the participating agency are being used, those IP Addresses, along with any related information, particularly PII, will be removed and US-CERT will analyze the situation and provide remedial actions.

US-CERT analysts will only see alerts and those portions of the participating agency's traffic that are captured due to their association with known or suspected cyber threats based upon the pre-defined signatures and scenarios; they will not have access to other redirected agency traffic. US-CERT will develop and operate signatures and scenarios according to written procedures to ensure that such signatures and scenarios deployed during the Exercise are based upon known or suspected cyber threats and collect only that content which is needed by US-CERT to detect, analyze, respond to, or prevent the cyber threat.

In the event US-CERT detects false positives generated by a particular signature, US-CERT will document the signature that generated the false positives, the nature of those false positives including the specific information generated by the faulty signature (particularly if that data includes PII) and the removal or modification of the signature and the aging out of the associated data. US-CERT will modify or remove the signature to eliminate the false positive.

When an alert is triggered based upon a signature, the connection event (communication between two computers) is captured. For example, if the alert is triggered by malicious code contained in an attachment to an email, that email will be captured. In many cases, the analysis of this event will only require looking at the attachment and not even reviewing the contents of the email. However, sometimes the malicious payload is hidden and delivered via the content (or body) of the email. In those circumstances, the analyst focuses on analyzing the event for the malicious payload, not on any content nor PII contained in the event. This process is also described on page 15 of the EINSTEIN 2 PIA[1].

Except for the use of classified signatures, the additional capabilities being tested during the Exercise will not generate any more information to be shared with DHS components than is currently the case with EINSTEIN 2. The use of the IPS capability and the automated alerts are

[1] For additional information see the EINSTEIN 2 PIA at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf.

both focused on additional ways to use the information related to cyber threats, not to generate additional data to share with DHS Components.

Uses of the System and the Information

Describe how the uses of the personally identifiable information have changed with this update and whether any privacy risks exist as associated with such changes.

The participating agency's traffic will be collected, used, disseminated or retained during Exercise operations in furtherance of DHS' cybersecurity and infrastructure protection responsibilities. In furtherance of those responsibilities, the Exercise will demonstrate: (1) the ability of a TICAP to redirect verified agency traffic through equipment owned and operated by DHS; (2) the ability of US-CERT to analyze redirected traffic to detect known or suspected cyber threats, and to respond appropriately to known or suspected cyber threats; (3) the ability of US-CERT to develop techniques for supporting future EINSTEIN enhancements; (4) the ability of US-CERT to generate automate alerts of identified known or suspected cyber threats; and (5) the ability to send the traffic back to the TICAP to be delivered to the participating agency in a timely and efficient fashion.

The Exercise technology will contain the following components:

Intrusion Detection Systems (IDS). The Exercise will use the existing EINSTEIN 1 IDS capability to scan network flow records and the EINSTEIN 2 IDS capability to use signatures to scan network traffic, for indicators of known or suspected cyber threats. Flow records are records of connections made to an agency's IT systems. Flow records identify: the source Internet Protocol (IP) address of the computer that connects to the federal system; the port the source uses to communicate; the time the communication occurred; the federal destination IP address; the protocol used to communicate; and the destination port. Signatures are specific patterns of network traffic that affect the integrity, confidentiality, or availability of computer networks, systems, and information. Examples of flow records and signatures are provided in the below Appendix as well as the publically available EINSTEIN 2 PIA. The Exercise technology will also include a second IDS. This IDS performs the same function as the existing EINSTEIN 2 IDS, except with greater speed and processing power. US-CERT will load signatures on both IDS systems.

Classified Signatures. These signatures will be used in both of the Exercise technology IDSs and will operate the same way and follow the same architecture as the signatures currently in use through EINSTEIN 2. These classified signatures trigger on indicators of known or suspected cyber threats and may be potentially derived from numerous sources, including any of the multiple agencies that engage in computer network security. All signatures, whether classified or unclassified and regardless of the source, are reviewed and approved by US-CERT prior to being deployed in the Exercise based on its written policies and procedures. Classified

signatures will provide US-CERT the capability to help the federal government defend against high impact threats.

Storage. US-CERT will store the IDS alerts and traffic related to known or suspected cyber threats for analysis.

Intrusion Prevention System (IPS). This system identifies known or suspected cyber threats and responds appropriate to the threat in a manner pre-programmed by US-CERT based on the threat. The Exercise will add a new component to existing EINSTEIN capabilities because it will allow the Exercise technology to affect redirected agency traffic in real time.

Automated Alerts. The Exercise technology will enable US-CERT to generate automated alerts announcing the detection of particular cyber threats, faster than the current manual process. The Exercise technology will process pre-programmed scenarios developed by US-CERT. US-CERT will determine which conditions will trigger an alert and program those conditions into the pre-defined scenarios.

The Exercise will also include the generation of reports of observed cyber threats. The network flow records, signatures, alerts, and portions of network traffic associated with cyber threats will be used by trained US-CERT analysts to identify and respond to computer network security incidents and anomalies, improve network security, generate reports for distribution to participating agencies and other partners, and increase the resiliency of critical, electronically delivered government services. Only information that is necessary to understand the reports or further the DHS cybersecurity mission will be included in any of these products.

The IDS and IPS capability used in the Exercise do not, in themselves, contain any analytical tools. All analysis of cyber threat related data during the Exercise will use commercial, government-provided, and in-house network security tools used to analyze instances of cyber threats detected to or from the participating agency's computer network - the same type of tools described in section 2.2 of the EINSTEIN 2 PIA. Many of the tools will be the same tools that are currently used in commercially available computer security software and those used by other federal executive agencies. These tools provide different ways to view, correlate, or compare the limited data generated by the signatures. US-CERT will use these tools during the Exercise to fulfill its responsibilities to detect and reduce computer network threats and vulnerabilities; disseminate computer network security threat and warning information; and, coordinate incident response activities.

The Exercise will not use commercial or publicly available data about individuals. The Exercise may use commercially provided signatures. Signatures may be derived from numerous sources such as: commercial or public computer security information; incidents reported to the US-CERT; information from federal partners; or independent in-depth analysis by the US-CERT – the same sources used in EINSTEIN 2 and in section 2.3 of the published EINSTEIN 2 PIA. All signatures will be reviewed and approved by US-CERT in accordance with its written

procedures. Analysts at the US-CERT may combine the EINSTEIN 2 data with other commercial or publicly available data, including information about Internet routes, bandwidth, and outages to create better situational awareness. The US-CERT does not focus on the identities of specific individuals and any data obtained from data providers will be limited to information relevant to the DHS cybersecurity mission.

In order to ensure that US-CERT personnel will only use data obtained during the Exercise for cybersecurity purposes, US-CERT has limited the data made available to US-CERT analysts to providing data associated with cyber threats as controlled through the signature and scenario approval processes and information handling procedures. In addition, the US-CERT maintains specific information handling requirements dictating that selection terms used for queries or searches of the data collected in response to signatures by US-CERT during the Exercise shall be based upon characteristics associated with cyber threats. Selection terms shall also be designed to result in the return of only data necessary for US-CERT analysis and to minimize the return of unnecessary PII. These protections are further reinforced through the oversight procedures of the Oversight and Compliance Offices of US-CERT, CS&C as well as being subject to review by the DHS Privacy Office and Office for Civil Rights and Civil Liberties.

Retention

Describe whether retention schedules have changed or if the system now has an approved National Archives and Records Administration schedule.

US-CERT will only retain network flow records, alert data, and those portions of the participating agency's traffic associated with cyber threats, reports and other products generated as a result of cyber threats detected during the Exercise. US-CERT will store this information in a protected system on a protected network accessible to only authorized US-CERT personnel with a need to know the information.

Data obtained by US-CERT in the course of the Exercise will be maintained for the minimum time necessary. Consistent with NARA General Records Schedule (GRS) 20, item 1a, the data may be retained for one year after the conclusion of the Exercise. Data obtained by US-CERT in the course of the Exercise will be purged within one year from the conclusion of the Exercise or earlier if US-CERT determines that particular data is no longer reasonably necessary for administrative, legal, audit or other operational purposes. No agency traffic is collected or retained by US-CERT unless it is associated with a cyber threat. Other agency traffic is not stored.

US-CERT analytic products, documents, and files generated in connection with the Exercise will be kept in accordance with DHS policy regarding retention of federal records. The current proposed DHS retention schedule for computer security incident handling reporting and

follow-up records states that all records are "temporary" and should be deleted or destroyed within three years after all necessary follow-up actions have been completed.

Internal Sharing and Disclosure

Describe how the internal sharing and disclosure have changed with this update and whether any privacy risks have been identified and if they have, mitigation for such risks.

If, during the Exercise, US-CERT shares network security information with other DHS components, it will do so consistent with its information handling procedures. Information about known or suspected cyber threats collected, analyzed, or otherwise obtained by US-CERT may be disclosed for cybersecurity purposes and in furtherance of the DHS cybersecurity mission.

In order to ensure that information is not inappropriately shared with internal DHS entities, US-CERT will implement information handling procedures including the substitution of specific PII with a generic label such as "PII." If the specific PII is necessary to understand the cyber threats, US-CERT will follow the information with a marking that indicates the sensitivity of that information such as "PII" and the document itself would be marked as including PII to further alert the recipient of the sensitivity of the included information.

External Sharing and Disclosure

Describe how the external sharing and disclosure have changed with this update and whether any privacy risks have been identified and if they have, mitigation for such risks.

The participating agency currently has access to network flow records through its participation in the use of the EINSTEIN 1 system. The agency will not be given access to the Exercise network flow records or alert data. The decision not to share Exercise network flow records or alert data with the participating agency was to keep the Exercise focused and to avoid building extraneous technical functionality such as the mechanisms needed to enable access to the network flow records.

US-CERT may share network security information with other external organizations consistent with its information handling procedures. Information about known or suspected cyber threats collected, analyzed, or otherwise obtained by US-CERT may be disclosed for cybersecurity purposes and in furtherance of the DHS cybersecurity mission.

Information collected by US-CERT during the Exercise may be disseminated for non-cybersecurity purposes—including law enforcement, intelligence, or administrative purposes—when the recipient is a federal, state, or local law enforcement entity and the information appears to indicate involvement in activities which may violate laws which the recipient is responsible to enforce or an agency of the federal government authorized to receive such information in the performance of a lawful government function. Such a dissemination must comply with the

Privacy Act and any other applicable statutes, regulations, or DHS policies. Any dissemination of information for non-cybersecurity purposes during the Exercise must be approved by the US-CERT Director or Deputy Director and the Office of the General Counsel.

If a particular communication includes content that describes criminal activity, that traffic will not be collected by the EINSTEIN 2 or the Exercise technology unless that traffic also happens to be associated with cyber threats for which there is an approved signature or scenario. US-CERT will share data for cybersecurity or non-cybersecurity purposes in accordance with written US-CERT procedures. While US-CERT does not engage in attribution, US-CERT may share information with law enforcement and intelligence organizations that may engage in attribution, particularly for these incidental criminal information. In all cases, US-CERT will remain available to clarify the meaning of the data it sends.

Notice

Describe whether additional notice is required to describe new collections, uses, sharing, or retention of the data and how that has or will be done.

The decision to use the participating agency's network or communicate electronically with the agency is essentially the decision to provide network flow records and the other network traffic that will be scanned with the Exercise technology.

Once an individual decides to communicate with the agency electronically, the network traffic will be subject to computer security efforts of US-CERT, including in this case the Exercise system, in addition to any individual computer security programs the participating agency might have in place. This situation is also described in the EINSTEIN 2 PIA.

Notice is provided to the public through the agency's website privacy policy which states that the agency uses computer security programs to monitor network traffic.

Individuals inside the participating agency's network receive notice by the agency's use of log-on banners and user agreements notifying agency personnel that their communications or data transiting or stored on the agency network and that network traffic is subject to monitoring and that traffic may be disclosed for network security and other lawful government purposes.

Notice was provided to users of the participating agency networks. In the MOU with DHS, the agency certified that it provides log-on consent banners or notices, terms of use policies or user agreements, computer training programs, or other mechanisms to notify users that the government routinely monitors communications occurring on agency networks for purposes including network operations and employee misconduct, law enforcement, and counterintelligence investigations; that the government may monitor, intercept, search, and seize communications transiting or stored on agency networks for any lawful government purpose; and that communications or data may be disclosed or used for any lawful government purpose.

It is a common risk that not all Internet communications reach their final destination due to many technological factors. While not a technical mitigation, this PIA provides awareness that US-CERT may affect the participating agency's traffic during the Exercise. This specific notice is supported by the general notice on the agency's website privacy policy that computer software is used to monitor network traffic. This risk will be further mitigated by US-CERT's written procedures that require US-CERT to take only those steps necessary to detect, analyze, and respond to a known or suspected cyber threat.

The sufficiency of the notice to users of an agency information system was discussed, in the EINSTEIN 2 context, by the U.S. Department of Justice Office of Legal Counsel in an opinion entitled, "Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch," dated August 14, 2009, and available on the Department of Justice's website: www.justice.gov/olc/2009/legality-of-e2.pdf. The U.S. Department of Justice issued a related Memorandum entitled, "Legal issues relating to the testing, use, and deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch", dated January 9, 2009, available: www.justice.gov/olc/2009/e2-issues.pdf. In accordance with standing OMB privacy policies, the participating agency also includes a privacy statement on its publicly facing websites which advises visitors generally how the agency manages and uses the information transmitted to its website and specifically that their interaction with federal networks is subject to monitoring for computer network security purposes.

Individual Access, Redress, and Correction

Describe how access, redress, and correction have changed with this update and whether any privacy risks have been identified and if they have, mitigation for such risks.

The Exercise has a narrow focus on cyber threats, not individuals, and results in the collection of a limited amount of information: just network flow records, alert data, and the agency traffic associated with cyber threats. The combination of the limited range of data collected (narrowly selected portions of network traffic that are directly linked to cyber threat) and the use of that data to detect and possibly prevent cyber threats will result in the minimal amount of information that could be considered PII and thus a minimal amount of information about which an individual would seek access, redress, or correction.

There is no formal redress or access mechanisms available as part of the Exercise.

There are no separate procedures for individual correction of information since network flow records, alerts, and agency traffic captured due to its association with cyber threats is generated from exact copies of computer network traffic. This same situation is described in section 7.2 of the EINSTEIN 2 PIA.

While section 7.1 of the EINSTEIN 2 PIA explains the FOIA process by which individuals can request information about the unclassified US-CERT network security activities and the EINSTEIN program, the Exercise will use classified systems and signatures and records that are properly classified pursuant to Executive Orders and are protected from FOIA disclosures pursuant to 5 U.S.C. § 552 (b)(1).

Technical Access and Security

Describe how the technical access and security have changed with this update and whether any privacy risks have been identified and if they have, mitigation for such risks.

Access to the Exercise system and related stored data is strictly limited to trained US-CERT personnel and contractors who are governed by policies and procedures. US-CERT contractors will have access to the Exercise systems and are subject to the same training, auditing, and oversight that govern the DHS employees.

All DHS employees are required to have general privacy training. In addition, US-CERT analysts and other persons who will participate in the Exercise information will receive training on privacy, legal, and policy issues.

The Exercise technology will be located on a protected network and physically located in a secure facility. A record for every signature and scenario shall be created and formally maintained by US-CERT that documents, at a minimum, the identified cyber threat, derivation, justification, and the intended effect and operation and the value of any portion of network traffic collected by the signature, as well as any applicable use instructions, use precautions, or sunset dates for the signature or scenario.

All external reports will be reviewed for appropriate information handling of PII according to written information handling standard operating procedures. All Exercise information will reside in a secured storage system.

All activities during the Exercise, both technical and personnel, will be subject to review by the Oversight & Compliance Offices of US-CERT and CS&C as well as the DHS Privacy Office and the Office for Civil Rights and Civil Liberties.

Technology

Describe how the technology has changed with this update and whether any privacy risks have been identified and if they have, mitigation for such risks.

The Exercise system was developed using DHS approved system engineering and development procedures, consistent with DHS Software Engineering Life Cycle (SELC) and Acquisition Program Management Director (APMD) processes and procedures.

The Exercise will operate in a classified environment thus preventing unauthorized access to system information. Access to the Exercise systems will be limited to individuals who are cleared at the appropriate security level and have received DHS Privacy Training.

Responsible Official

Randall Vickers
Acting Director, US-CERT (888) 282-0870
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix: Examples of Network Flow Records and Signatures

The following examples are copied from pages 7 – 9 of the EINSTEIN 2 PIA.

Sample network flow records

127.0.0.1|192.168.0.20|52119|25|6|10|600|S|2008/04/28T00:02:47.958|44.985|2008/04/28T00:03:32.943|SENSOR1|out| S|sIP|dIP|sPort|dPort|protocol

|packets|bytes|flags|sTime|dur|eTime|sensor|type|initialFlags|

Explanation of Sample network flow records (all Samples Unclassified) :

- 127.0.0.1 (sIP) IP of Computer who is the source of the connection
- 192.168.0.20 (dIP) IP of the computer who is the destination of the connection
- 52119 (sPort) Port the connection was initiated on by the source computer
- 25 (dPort) Port the connection was received on by the destination computer
- 6 (protocol) Protocol number, the number is based on the protocol being used to transport the data (6 = TCP, 1 = ICMP, 17 = UDP)
- 10 (packets) Count of total number of packets seen in this single connection (calculated by the sensor)
- 600 (bytes) Count of total number of bytes seen in this single connection (calculated by the sensor)
- S (flags) Aggregation of all flags seen in this single connection. Flags describe what happened in the connection
- 2008/04/28T00:02:47.958 (sTime) Start time of the connection, Universal Timestamp added by sensor to indicate when the connection was started
- 44.985 (dur) Duration of the connection, this field is calculated (dur = eTime - sTime)
- 2008/04/28T00:03:32.943 (eTime) End time of the connection, Universal Timestamp added by sensor to indicate when the connection was ended
- SENSOR1 (sensor) Name of the Sensor that collected the data, this field is added by the sensor
- out (type) Direction of the traffic (types include “in,inweb,inicmp,out,outweb,outicmp, int2int,ext2ext")

- S (initialFlags) First flag seen in the connection, this is only based on the first packet of the connection
- Flag Markers and their meanings
- C = CWR - Congestion Window Reduced
- E = ECE - Explicit Congestion Notification echo U = URG - Urgent A = ACK - Acknowledgement P = PSH - Push R = RST - Reset S = SYN - Synchronize F = FIN – Finished

Sample Signature

For illustrative purposes only, the following is an example of a commercially available signature. (This is not a signature the 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;)
```

Explanation of Signature:

- Alert: Type of IDS Event
- tcp: Protocol being examined
- any: Any source IP
- any: Any source port
- ->: Direction (points to @HOME_NET which indicates inbound)
- $HOME_NET: A variable which is defined by the IDS as the subnets that make up the internal network 443: Destination port traffic is bound for
- msg:"DoS Attempt": Name of the alert that is sent to the console (for humans reading the alert console)

The remaining fields of the string tells the IDS what to look for, the breakdown of the commands and instructs the IDS where in the packet to look for the text.

This signature example tells the IDS to alert on any external IP on any external port that sends traffic to the home network, on port 443, with the text “|16 03 00|”, and the text “|01|” within certain parameters and offsets. The alert name is defined as “Dos Attempt” and references CVE, SID:2000016, revision 5.