Privacy Impact Assessment
EINSTEIN Program

Collecting, Analyzing, and Sharing Computer Security Information Across the Federal Civilian Government

Department of Homeland Security
National Cyber Security Division
United States
Computer Emergency Readiness Team
(US-CERT)

September 2004

PRIVACY IMPACT ASSESSMENT

EXECUTIVE SUMMARY

- This Privacy Impact Assessment (PIA) examines the privacy implications of the United States Computer Emergency Readiness Team's (US-CERT's) EINSTEIN Program in accordance with Section 208 of the E-Government Act and the guidance for PIAs issued by the Office of Management and Budget (OMB). This PIA addresses for the EINSTEIN Program:

    - What and why the information is being collected;
    - The intended use of the agency information;
    - With whom the information will be shared;
    - What notice or opportunities for consent would be provided to individuals regarding information collected;
    - How that information is shared and secured; and
    - Whether a system of records is being created under section 552a of title 5, United States Code (the "**Privacy Act**").

- The EINSTEIN Program is an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government. By collecting information from participating Federal government agencies, the US-CERT builds and enhances our nation's cyber-related situational awareness. Awareness will facilitate identifying and responding to cyber threats and attacks, improve network security, increase the resiliency of critical, electronically delivered government services, and enhance the survivability of the Internet.

- The US-CERT has prepared the EINSTEIN Program to implement statutory and administrative responsibilities in two distinct, but related areas.

    - First, in accordance with the mandate of the Homeland Security Act, as well as of Homeland Security Presidential Directive 7, the Department of Homeland Security (DHS) through the US-CERT will deploy the EINSTEIN Program to help protect cyberspace.
    - Second, in accordance with the Federal Information Security Management Act ("**FISMA**"), the EINSTEIN Program supports Federal agencies in their efforts to comply with Congressional requirements for information security, including compliance with information assurance guidelines prepared by OMB. The EINSTEIN Program provides an essential layer of protection for the Federal Enterprise Architecture ("**FEA**") and the IT infrastructure used to deliver essential citizen services. There are no other cross-agency, automated processes that support FISMA compliance, protect the FEA, and focus on delivery of essential government services.

- In this manner, the EINSTEIN Program supports Federal agencies' efforts to protect their computer networks. System and network administrators within each agency are responsible for guarding access to sensitive information and computing infrastructure. During the past several years, network attacks and disruptions have become increasingly common and occur at rates that prevent government officials from managing risks effectively without a collective and collaborative information-sharing program. Both

statutory provisions and the Office of Management and Budget require agencies to share incident and risk data with the US-CERT to accomplish these goals.

- Federal agency partners are the core of the EINSTEIN Program's capability. Each Federal agency administrator retains complete control of network data in strict accordance with Federal laws and polices. Agencies gather and subsequently share security data directly with the US-CERT, based on reporting requirements established by OMB. In turn, the US-CERT prepares a strategic, cross-agency assessment, which is then shared back with all Federal civilian agencies. Federal civilian agencies are -- in return for sharing anomaly and security data -- better positioned to protect their systems, save scarce resources, and provide essential services.

THE EINSTEIN PROGRAM

Introduction

Because we live in a world dominated by computers and the Internet, protection of cyberspace is of critical importance to this nation's national security, economic well-being, public safety, and the protection of personal information maintained in electronic databases. This is especially true at the Federal agency level where relationships between citizens and their Government have been and will continue to be transformed by technology.[1] These advances have allowed agencies to enhance their functions and services, achieve efficiencies, and increase transparency and access.

With the clear benefits from technology, however, has come an increased awareness of the potential vulnerabilities of the Federal information infrastructure. It is critical to assess and manage cyber risks at the federal agency level in order to ensure the delivery of government services, whether in times of calm or under national alert. Experience has demonstrated, moreover, that protecting federal cyberspace requires a cross-government awareness of issues and collaborative management.

The Role of DHS and US-CERT

Federal policy recognizes the importance of an enterprise solution for cybersecurity. Appropriately, the Director of the Office of Management and Budget (OMB) is required by FISMA to oversee Federal agency information security policies and practices and to coordinate a comprehensive, government-wide, risk-based approach for managing information security issues. FISMA additionally requires OMB to oversee the operation of a central Federal information security incident center, the function of which is now housed in NCSD's US-CERT. OMB provides guidance to Federal agencies on incident identification and reporting.[2]

---

1 In fact, the E-Government Act of 2002 was enacted to promote federal use of technology as a primary means to access high quality Government information and services across multiple channels and to make the Federal Government more transparent and accountable. Section 208 of that statute requires the preparation of privacy impact assessments for information technology that collects, maintains or disseminates information that is in an identifiable form.

2 The US-CERT function is the central activity for the collection and analysis of reports detailing cyber events impacting Federal information technology (IT) resources. The US-CERT mission is, inter alia, to assist

FISMA places responsibility on multiple levels of each agency to support government-wide incident identification and reporting. The creation and maintenance of incident reporting processes raise managerial as well as technical issues. Agency heads, senior program officials, agency CIO's, Inspectors General, and other security professionals are each part of an overarching and integrated process to define, maintain, continuously improve, and certify incident reporting requirements. Inherent in this responsibility are requirements to develop incident identification and reporting processes that reflect an understanding of both agency-specific risks as well as risks that are generated by shared infrastructures and systems.

Significantly, the Homeland Security Act establishes a primary role for the Department of Homeland Security in coordinating this enterprise solution through crisis management for cyberspace security. Within DHS, the National Cyber Security Division (NCSD) serves as the Federal government's cornerstone for cyber security coordination and preparedness. The operational arm of the NCSD is the United States Computer Emergency Readiness Team (US-CERT), a partnership between NCSD and the public and private sectors that has the responsibility to:

- Compile and analyze information security incident information;
- Inform agencies about information security threats and vulnerabilities; and
- Consult with national security agencies and operators of national security systems to promote cyber security best practices and preparedness.

As a central repository of incident information, the US-CERT has a responsibility to present a single, government-wide focus for monitoring and evaluating risk management and assessment activities based on identified government priorities, functions, and services. Only through an active information exchange on incidents and activities can the government implement the information security objectives in FISMA. In summary, US-CERT carries out these responsibilities by obtaining and analyzing information and data from Federal agencies, and disseminating timely, actionable information based on that analysis.

The EINSTEIN Program

Most of the Federal government's Internet-based services are provided separately by each agency within individual agency jurisdictional boundaries and in the context of individual agency cultures and unique information systems. Proper management of cyber risks, however, requires that Federal civilian agencies work collaboratively on information security issues and challenges in order to foster situational awareness. Situational awareness involves the ability to identify, process, and comprehend the critical elements of information related to an area of interest -- in this case, cybersecurity. Building situational awareness to help protect federal information systems (and help them protect themselves) and cyberspace, generally, requires input in the form of information and data from federal agencies.

Currently, information sharing from Federal agencies to the US-CERT about cyber vulnerabilities and incidents occurs manually and inconsistently. There are no established processes for automating information sharing about cyber incidents; instead, the information exchange that does occur happens primarily after the fact, when multiple systems in the Federal

---

Federal agencies and departments in securing their cyberspace.

infrastructure already may have been affected. Experience with recent cyber attacks has demonstrated that effective defenses require accelerated information sharing, analysis, and enhanced response preparation.

The lack of any meaningful system to test or monitor system activity across all Federal agencies in real-time places individual agency systems and operations at risk. Because of our cyber interdependence, IT weaknesses associated with any single Federal agency can affect the security of the entire Federal government. Put another way, our interconnected network of information systems has made each agency only as secure as the security of our weakest link. This underscores the importance of cross-governmental information security collaboration. Effective implementation of FISMA requires robust incident identification and reporting across all of the government agencies.

US-CERT has therefore created the EINSTEIN Program to help agencies more effectively protect their systems and networks. The EINSTEIN Program is an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal civilian government so that Federal agencies will be aware, in near real-time, of the threats to their infrastructure and can act swiftly to take corrective measures.

The cornerstone of the EINSTEIN Program is the ability to generate and report necessary IT-related information from the Federal agencies in a timely and appropriate manner. Given the record of inconsistent and incomplete agency reporting to date, it is essential that agencies respond to OMB requirements to report to the US-CERT. Although the incident and security information that is currently collected by Federal agencies can provide some value, to truly enhance the security of Federal information systems consistent with FISMA and OMB expectations, agencies must contribute to a common pool of useful, actionable, situational awareness.

Agency and network administrators will also benefit from services provided by cross-agency and collaborative benefits generated from the EINSTEIN Program. Ultimately, each agency must undertake responsibility for developing an appropriate risk management and security program at the department or agency level. Of OMB's Six Common Security Weaknesses, agency administrators are responsible – at a minimum – for detecting, reporting, and sharing information on vulnerabilities.[3]

OMB: Six Common Security Weaknesses

1. Senior Management Attention
2. Measuring Performance
3. Security Education & Awareness
4. Funding and Integrating Security into Capital Planning and Investment Control

3 The EINSTEIN Program is structured to support resolution of the six common IT security weaknesses identified by the OMB in multiple ways. This is true of the sixth weakness – detecting, reporting, and sharing network vulnerabilities -- but also other weaknesses. For example, the automated incident and reporting capability can also secure contractor operations. Most importantly, however, the EINSTEIN Program offers, for the first time, an ability to measure performance with regard to complex IT security issues. In the area of privacy protection, for example, the capability can measure whether and the extent to which sensitive data is being improperly accessed, secured, or at risk because of other reasons.

5. Ensuring that Contractor Services are Adequately Secure
6. Detecting, Reporting, and Sharing, Information on Vulnerabilities

However, the capability provides several additional benefits for system and network administrators to help address common security weaknesses and promote the cyber security of government systems. These include each of the following:

- **Worm Detection**: Sharing and collaborating on IT incidents, threat, and vulnerabilities produces a sophisticated picture of attacks across the Federal .gov domain. The US-CERT provides this information directly to network administrators for the benefit of department and agency systems protection.
- **Anomalous Activity** – In- and out-bound: Similarly, in culling out certain cross-agency indicia – such as known criminal behavior or traffic that is highly suggestive of criminal behavior – the capability offers directly to the department and agency administrators an easy to understand picture on priority emergencies and needs. In the absence of such information, administrators must continue to rely on insufficient information to leverage scarce resources and to protect their systems.
- **Configuration Management**: The US-CERT will be able to provide counsel on configuration management options. Configuration challenges are fast becoming one of the most difficult problems for agency administrators. The EINSTEIN Program offers information and options – based on a collective and collaborative approach.
- **Trends Analysis**: The US-CERT uses the information collected and analyzed to generate a cross-governmental trends analysis. The analysis offers to departments and agencies an accurate and aggregate picture on the health of the Federal.gov domain. The information is offered in real-time, and may include an assessment of anomalous amounts of network traffic across the .gov domain – or, in some cases, within a single agency. The data can also offer an aggregate comparison on the health of the Federal .gov domain as compared to the Internet or even portions of the national network.

REASONS FOR INFORMATION COLLECTION

OMB requires that Federal civilian agencies report cyber incidents to the US-CERT. The EINSTEIN Program provides an efficient and cost-effective way to comply with legal requirements and protect critical systems. In operating the EINSTEIN Program, the US-CERT will significantly strengthen the security posture of the federal government. US-CERT will provide both technical support and program management.

US-CERT analysis will provide agencies with a better understanding of their current security status as it relates to the overall government security status and the status of Internet security generally. In addition, agencies will be able to perform analyses that will help to increase the security and understanding of potential security problems on their networks. The EINSTEIN Program will help agencies identify baseline network traffic patterns, configuration problems, unauthorized network traffic, network backdoors, routing anomalies, and network scanning activities.

The EINSTEIN Program will provide the US-CERT and Federal agencies with a capability to detect behavioral anomalies within their networks. By analyzing the data and detecting these anomalies, the ability to detect new exploits and attacks in cyberspace will be

greatly increased. Enhancing the ability to act swiftly in today's rapidly changing electronic environment is essential to protect government systems.

The following are examples of the various analytic processes and products that the EINSTEIN Program will produce to protect the participating Federal agencies:

- Determine the scope and impact of any specific worm across the Federal government and how it relates to the Internet community at large;
- Detect anomalous network behavior or activities against the Federal government and determine whether it's a focused attack or part of a larger Internet-related activity;
- Determine the level of impact and any damage associated with cyber attacks against the Federal government;
- Diagnose specific Federal agency Internet traffic problems as they relate to the much larger Internet backbone infrastructure;
- Pinpoint the apparent source responsible for any cyber-related attacks;
- Determine the cyber state of the Federal government in near real-time and its interaction with the global Internet community;
- Compile an overall situational awareness of trends and traffic patterns for all participating Federal agencies;
- Detect early warning and indications of emerging attacks and malicious reconnaissance activities and adverse impact on Federal government agencies; and
- Correlate system compromises within the Federal government.

What Information is to be Collected

When an individual uses the Internet to browse, read pages, download information or otherwise communicate with a Federal ".gov" website, pursuant to Federal law and policy, Federal agencies collect security and network information about these transactions. In order to collect this information legally, agencies must post security and privacy policies, which include notice about: use of cookies; collection of security and automated data; collection of email traffic and information from web forms; and collection of personal identifiers for service delivery purposes. Additionally, when personally identifiable information is collected, agencies are required to conduct privacy impact assessments ("**PIA**") analyzing the privacy implications of the collection.

The information associated with the collection of security and network information is created at the agency level and allows agencies to monitor their own network activity. The EINSTEIN Program will obtain certain portions of this data -- the portion needed to conduct analysis of the status of Internet traffic -- in near real time, in order to perform analysis and provide situational awareness for Federal agencies concerning the state of Internet traffic across the Federal .gov domain. The collection will be passive, that is, obtaining the data needed for analysis will not interfere with the communications to and from agencies.

The particular data to be collected are strictly limited, and are selected based on criteria for anomaly detection and other information technology risks. The data may include:

- Autonomous System Numbers (ASN). An autonomous system is a group of Internet Protocol (IP) networks that adhere to a single routing policy. An Autonomous System

Number (ASN) identifies the autonomous system -- networks using the same, specified routing policy -- and enables the autonomous system to exchange information with other autonomous systems.

- ICMP Type/Code. ICMP (Internet Control Message Protocol) is used to communicate control messages on the Internet between hosts/routers. ICMP packets can contain diagnostic (ping, traceroute), error (network/host/port unreachable), information (timestamp, address mask request, etc.), or control (source quench, redirect, etc.) messages. Although these messages are generally harmless, there are nevertheless some message types that should be dropped. Some ICMP messages can be used to redirect traffic from a web site. Other messages can leak information about a host that could be helpful to an attacker. ICMP messages are also sometimes used as part of DOS attacks (e.g., flood ping, ping of death).

- Packet Length. A packet is specially formatted group of bits containing data, IP address, and control information that is transmitted over a network as a collective unit. Messages are usually broken down into a sequence of several transmitted packets that are reconstructed for completeness at their destination. Different systems use packets of varying sizes, and abnormal or spikes in packet length, especially in light of the protocol being used, could be indicia of malicious activity.

- Protocol. A protocol is a standardized means of communication among machines across a network. Protocols allow data to be taken apart for faster transmission, transmitted, and then reassembled at the destination in the correct order. The protocol used determines the way errors are checked, the type of compression, the way the sender indicates the end of the transmission, and the way the receiver indicates that the message has been received. Protocols can describe low-level details of machine-to-machine interfaces (e.g., the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (e.g., the way in which two programs transfer a file across the Internet).

- Sensor identification and connection status. Sensor identification is the description of where the sensor is located so it is clear which network/system/agency the data is coming from. Connection status is simply whether or not the system is receiving information

- Source and Destination IP Address. Internet Protocol (IP) addresses are four octet (32-bit) source or destination addresses that uniquely identify computers either on a given network or on the Internet. Source identifies the device sending the packet; destination identifies the intended recipient.

- Source and Destination Port. In the networking world, the term ‘port’ is a number that identifies the beginning or endpoint of a logical connection. This number that is part of the URL (Internet address) right after the domain name. Every Internet protocol has a dedicated port -- for instance, file transfer protocol services channel information on port 21, HTTP services use port 80 and POP (or POP3) services use port 110. Internet protocols appearing on an unusual port number may be indicia of malicious activity.

- TCP flag information. Simply stated, a TCP flag is a piece of information that is added to packets traveling between computers that describes the status of the connection

between the computers. These 'flags' are very specific information, and any abnormality in the way they appear or are paired could be indicia of malicious activity.[4]

- Timestamp and duration information. A time that is printed to a file (such as email) or other location to help keep track of when data is added, removed, sent, received, etc.

The Intended Use of the Information

The information to be collected by the EINSTEIN Program will be used to provide the US-CERT and Federal agencies with the capability to detect and correlate anomalies across agency networks. These anomalies include configuration problems, unauthorized network traffic, network backdoors, routing anomalies, network scanning activities, and baseline network traffic patterns.

The process is as follows:

First, Federal civilian agencies will collect subject data. Each agency will transmit to a secure US-CERT facility only that data that meet the criteria for anomaly detection and other IT risks. The US-CERT has structured the program to limit the amount of data collected.

Second, the US-CERT will then analyze data submissions. Analysts are trained to identify anomalous activity and will strictly focus only on such activities.

Third, where there are suspicious anomalies or other aberrations, the US-CERT analysts will collaborate with agency partners to examine more carefully additional network activity associated directly with such activities.

Fourth, in addition to providing information about potential anomalies and other aberrations, EINSTEIN will also be able to offer agencies counsel on configuration management options. The EINSTEIN Program will offer information and options based on a collective and collaborative approach.

Situational information generated as a result of EINSTEIN will also allow the US-CERT to generate a cross-governmental trends analysis. The analysis will provide departments and agencies with an accurate and aggregate picture of the health of the Federal .gov domain in real-time, and an aggregate comparison of the health of the Federal .gov domain as compared to the Internet.

With Whom Will the Information Be Shared

The data generated by, and required to operate the EINSTEIN Program, will be shared between US-CERT and participating Federal agencies. The program is structured so that data is shared in increments. Certain categories of data, as explained above, will be collected. If anomalous activities are uncovered by the EINSTEIN Program, US-CERT will ask for additional information in order to ascertain the cause of the anomaly. Upon US-CERT's completion of an analysis of the necessary data, the results will be shared with a particular Federal agency or

4 Transmission Control Protocol is a set of rules that govern how computers 'communicate' with one another and how information is organize and sent between computers over the Internet.

agencies. Upon receipt of these anomaly reports, it will be up to each agency, consistent with its own information sharing practices, to decide if and how to act on the information. US-CERT will not share information obtained through the EINSTEIN Program beyond its agency partners, except to the extent that such information can be generalized as part of the alerts and warnings that are central to the US-CERT mission.

Notice and Consent

When personally identifiable information is collected by a Federal agency, that agency must comply with all relevant statutory and regulatory requirements relating to privacy protections. As an example, Federal agencies must post notices on their websites as well as at other major points of entry that computer security information is being collected. Such notices cover automated data collection, security and intrusion detection, and information collected from e-mails. Additionally, each Federal agency must publish PIAs covering personally identifiable data that may be collected.

The EINSTEIN Program does not in any way supersede or replace the privacy requirements in place for participating Federal agencies, based on information collected in the normal course of conducting operations. Although OMB enforces these privacy requirements, the US-CERT will be available to assist participating agencies in ensuring compliance.

Ensuring the Security of the Information

The US-CERT has structured the EINSTEIN Program to allow for an increase in the speed and quality of alerts and reports about the health of, and threats to, the Federal .gov domain to facilitate compliance with security requirements. The limited information sent to the US-CERT will be sent using a secured protocol (e.g., secure socket shell).

Access to the data is strictly limited to users on a need-to-know basis. The records will be maintained in an area subject to general building security, including physical and administrative safeguards. Any paper records and electronic records on CD-ROMS and floppy discs are stored in lockable metal cabinets in rooms locked during non-duty hours. The records stored in electronic media (electronic databases or CD-ROMS and floppy discs) are password protected. A schedule regarding the types of records to be stored, as well as the length that such records will be retained, is currently being prepared.

Creation of a Privacy Act System of Records

US-CERT has not prepared a system of records notice for the EINSTEIN Program because the program is not intended to collect information that will be retrieved by name or personal identifier. The primary focus of the program is at the network level. Accordingly, a system of records is not being created.

Conclusion

One of the main goals of the EINSTEIN Program is to improve the quality, quantity, and speed of sharing information. By participating in the EINSTEIN Program, Federal agencies will benefit by raising the cyber situational awareness for their individual agency, help meet their statutory requirements concerning information security, and contribute to the overall effort to

build the government cyber situational awareness. In addition, agency participation assists US-CERT in determining the best ways to help agencies protect themselves, and contributes to the ability of US-CERT to provide timely alert and warning information to government and the private sector.

Federal agency participation is paramount to the overarching situational awareness capabilities the EINSTEIN Program can offer and its collaborative benefits. The use of this automated analysis capability by the Federal civilian agencies represents one way that the US-CERT is leveraging current operational technology to significantly increase the overall situational awareness of our Nation's Cyberspace, as well as the Internet community at large.

* * *

Contact information: Questions or comments about this PIA should be directed to Thomas Dukes, Office of the General Counsel, DHS, Thomas.Dukes@dhs.gov, Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, nuala.kelly@dhs.gov. or Andy Purdy, Privacy Officer, NCSD, andy.purdy@dhs.gov.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu