Privacy Impact Assessment Update
for the

EINSTEIN 1: Michigan Proof of Concept

February 19, 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

The Department of Homeland Security ("DHS") and the State of Michigan ("Michigan") plan to engage in a 12-month proof of concept to determine the benefits and issues presented by deploying the EINSTEIN 1 capability to Michigan government networks managed by the Michigan Department of Information Technology (MDIT). This PIA updates the previous EINSTEIN PIAs (EINSTEIN 1 PIA from 2004 and EINSTEIN 2 PIA from 2008, both available on www.dhs.gov/privacy)[1] in one narrow aspect: the use of EINSTEIN 1 technology in a proof of concept with Michigan. This PIA update addresses the privacy impacts of extending the current EINSTEIN 1 functionality to Michigan in this specific proof of concept.

Introduction: The Michigan Proof of Concept

National Security Presidential Directive 54 ("NSPD-54")/Homeland Security Presidential Directive 23 ("HSPD-23") directed the Secretary of Homeland Security, in consultation with the heads of other sector-specific agencies, to submit a report detailing the policy and resource requirements for improving the protection of privately owned U.S. critical infrastructure networks. One of the recommendations contained in that report was for DHS to evaluate "the feasibility of sharing federally developed technology capabilities with the CIKR." Following a subsequent feasibility study and detailed coordination that considered policy, technical, legal and security issues, DHS and the State of Michigan agreed to a one-year pilot program during which the DHS EINSTEIN 1 capability would be deployed to specified Michigan government networks managed by the MDIT.

DHS selected Michigan to partner in this proof of concept because of its architecture and close working relationship with DHS. Because the MDIT centrally manages the security of many Michigan government networks, Michigan was an ideal candidate to conduct this proof of concept. Furthermore, Michigan works closely with DHS in many of its CIKR cybersecurity efforts including leadership in Information Technology Sector Government Coordinating Council activities and involvement in the DHS, State, Local, Tribal and Territorial Government Coordinating Council.

Pursuant to a Memorandum of Agreement between DHS and Michigan, the EINSTEIN 1 proof of concept between US-CERT and Michigan will only involve network flow records of traffic to and from government networks managed by the MDIT, and no Michigan government

[1] When the mechanisms and/or privacy protections are the same in both the EINSTEIN 1 and EINSTEIN 2 PIAs, the EINSTEIN 2 PIA will be cited given that it is more current and provides a more detailed discussion of the protections. Like EINSTEIN 1, EINSTEIN 2 passively observes network flow records while also monitoring network traffic, in near real-time, for the existence of known malicious activity through network intrusion detection system (IDS) technology that uses pre-defined signatures. EINSTEIN 2 enhances computer network security by providing real time alerts on specific malicious network activity to US-CERT. EINSTEIN 2 is not currently part of this proof of concept.

network traffic content will be provided to US-CERT.[2] US-CERT and the MDIT's analysis of Michigan network flow records will enable the identification of anomalies in the network traffic that may be indicative of malicious activities.

During the proof of concept, when US-CERT identifies anomalies based upon Michigan network flow records that may be evidence of potential malicious activity, US-CERT will notify the MDIT. This is the same process used with the existing EINSTEIN 1 capability between US-CERT and federal executive agencies. Based on the information provided by US-CERT, Michigan will be able to investigate the potential malicious activity. Michigan, but not US-CERT, could analyze its full network traffic associated with the anomaly. During the proof of concept, US-CERT will not have the ability to access the content of Michigan government traffic through EINSTEIN.

Michigan can use the information from US-CERT to confirm whether the anomaly is a known threat, a previously unknown threat, or a "false positive" anomaly that is not indicative of malicious activity. Michigan will thus be better positioned to identify and resolve a greater range of threats to its cyber infrastructure. The increased US-CERT insight into anomalies affecting state government networks will also enhance US-CERT's overall situational awareness and ability to identify threats that may affect other customers, including federal executive agencies, and enhance the cybersecurity of government and CIKR networks. The feedback US-CERT will receive from Michigan will thus enable US-CERT to provide earlier warning to the presence of newly detected threats so that all can be better protected. The MDIT can also independently analyze net flow records generated from the EINSTEIN I capability and alert US-CERT to potential malicious activity that it finds, further assisting US-CERT in the identification of malicious activities that can provide early warning of threats to other US-CERT customers. The aggregated and correlated insight will further reduce and prevent computer network vulnerabilities.

Following the implementation of EINSTEIN 1 with Michigan and a period of operational coordination, an assessment of the value of the proof of concept to US-CERT's mission and to Michigan will be conducted. That assessment will consider, among other factors, any challenges encountered in the proof of concept; further policy, technical, legal or security issues identified; and successes achieved, and may also include recommendations about further pursuing the concept with Michigan or other CIKR partners.

[2] This distinction between the EINSTEIN 1 and EINSTEIN 2 capabilities is also discussed EINSTEIN 2 PIA.

Reason for the PIA Update

Currently, US-CERT operates the existing EINSTEIN 1 system on behalf of federal executive agencies. During this proof of concept, US-CERT will offer similar EINSTEIN 1 service to Michigan in a manner that will benefit its service for US-CERT's existing federal executive agency customers. This PIA update modifies the existing EINSTEIN PIAs to address the privacy impact of implementing the EINSTEIN 1 capabilities on a state government network instead of a federal executive agency network.

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

EINSTEIN 1 was developed by DHS in 2003 and currently provides an automated process for collecting, correlating, and analyzing computer network security information from voluntary participating federal executive agencies. Just as with the coordination of EINSTEIN 1 with federal executive agencies, the proof of concept of EINSTEIN 1 with Michigan will enable US-CERT to analyze network flow records in order to detect anomalies that may be evidence of malicious activities threatening the security of government networks and systems.

Flow records are records of network connections made to state networks and systems. Net flow records identify:

- The source Internet Protocol (IP) address of the source computer involved in the data transaction;
- The port the source computer used in the communication;
- The time the communication occurred;
- The IP address of the destination computer involved in the data transaction;
- The protocol used to communicate; and the port the destination computer used in the communication.[3]

[3] EINSTEIN 2 PIA at 3. (Footnotes to the EINSTEIN 2 PIA are used throughout this PIA to highlight

Using network flow records, US-CERT can detect certain types of malicious activity and coordinate with the managers of the associated government networks to mitigate those threats and vulnerabilities. US-CERT shares the trend-level results of this analysis, along with additional computer network security information, with both the public and private sectors via the US-CERT web site.

The proof of concept will use the same limited data as is currently used in the federal deployment of EINSTEIN 1. Network flow records include IP addresses but it does not include any additional information that may identify the individuals communicating or the contents of their communication (see the below Appendix for an example of network flow record data).[4]

The proof of concept will not use the EINSTEIN 2 capability. That means that the proof of concept will not use the intrusion detection signatures and thus will not capture the type of network traffic captured by EINSTEIN 2. The only data associated with the proof of concept will be the limited information that constitutes flow records. DHS will conduct a new PIA or PIA update if EINSTEIN 2, or any other technology, is considered as part of this or a related proof of concept.

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 purpose of the proof of concept is to explore whether the concept being undertaken is of value in the effort of improving the protection of state government networks by leveraging federal government developed technologies and capabilities.

In the proof of concept, US-CERT will analyze government network flow records from Michigan in addition to those other federal executive agencies currently leveraging US-CERT's analytical capabilities. Michigan may also analyze its network flow records obtained from the EINSTEIN 1 system. Michigan's analysis will enable both US-CERT and Michigan to identify anomalies in the network flow records that may be indicative of malicious activities. Some of those malicious activities may be known and others may have been previously unknown.

During the proof of concept, when US-CERT notices anomalies that may be evidence of potential malicious activity it will alert Michigan and Michigan may then investigate the activity. Separately, Michigan, as the owner and manager of its networks, maintains access to the full network traffic (as opposed to US-CERT which will only access the flow record data) and can

---

consistencies between this proof of concept and the existing EINSTEIN program and privacy protections. While the EINSTEIN 1 PIA includes more technical information about the EINSTEIN 1 capability, the EINSTEIN 2 PIA provides more information regarding the broader privacy considerations integrated into the EINSTEIN program.)

[4] EINSTEIN 2 PIA at 10.

analyze the network traffic information associated with the network flow data to confirm whether the anomaly is a known threat, a previously unknown threat, or a 'false positive' anomaly that is not indicative of malicious activity. Michigan's independent decision to investigate and then subsequently provide feedback to US-CERT will provide US-CERT alert/warning to the presence of new threats which US-CERT can then publish to its customers to enable other government networks and systems to be better protected.

From a privacy perspective, the only difference between the existing EINSTEIN 1 implementation with federal executive agencies and the DHS-Michigan EINSTEIN 1 proof of concept is the fact that Michigan is a state instead of another federal executive agency.

Under the current operational concept, Michigan can limit US-CERT access to Michigan's network flow records and may terminate the proof of concept at any time. While Michigan may choose to report the results of its independent analysis, US-CERT will not be able to access any data beyond the EINSTEIN 1 network flow records or other information specifically made available by Michigan.

The DHS-Michigan Memorandum of Agreement ensures that Michigan will notify DHS of any changes to handling or security requirements governing the network flow records transacted between them. The agreement also requires that all network flow record transactions between US-CERT and Michigan pursuant to the proof of concept be encrypted.

During the proof of concept, US-CERT will only use the network flow records to conduct analysis designed to identify indications of malicious computer network activities. This will assist Michigan in their existing and ongoing internal computer network security operations.[5]

No computer network traffic to or from Michigan's network will be interrupted by the EINSTEIN 1 technology used in the proof of concept.[6]

No commercial or publicly available data about individuals will be accessed, captured, maintained, or otherwise used in this proof of concept.[7]

US-CERT may use commercial or publicly available data about Internet routes, bandwidth, and outages to create better situational awareness as they analyze the flow records associated with this proof of concept.[8]

---

[5] This is the same limited use described on page 8 of the EINSTEIN 1 PIA. US-CERT's overall uses and analytical tools discussed in the "use" section on pages 11-13 of the EINSTEIN 2, and the correlating section of the EINSTEIN 1 PIA also apply to the proof of concept.

[6] EINSTEIN 2 PIA at 12.

[7] EINSTEIN 2 PIA at 12.

[8] EINSTEIN 2 PIA at 12.

Any specific references in the EINSTEIN 2 PIA to the use of signatures does not apply to this proof of concept since US-CERT will not be deploying signature-based capabilities and will only be undertaking network flow record analysis.

Only trained and experienced computer network professionals will have access to the system and data and they will be subject to oversight and audits.[9]

Retention

Describe whether retention schedules have changed or if the system now has an approved NARA schedule.

Network flow records collected from Michigan government networks managed by the Michigan Department of Information Technology (MDIT) will be maintained for the duration of the proof of concept and will be archived at the conclusion of the proof of concept and provided to the Michigan Department of Information Technology.

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.

During the proof of concept, US-CERT may use the network flow records obtained to produce similar high-level reports to those described on page 14 of the EINSTEIN 2 PIA, enabling notification of anomalous or suspicious activities to federal executive agencies and Michigan. The network flow record data obtained during this proof of concept may be combined with the analyses of other network flow records currently analyzed as part of the EINSTEIN program. US-CERT will not include any attribution in the reports it may generate as part of this proof of concept. [10] The limited nature of these reports is further reinforced by the limited information contained in network flow records.

All reports will be limited to publishing network flow records indicators of malicious computer network activity.[11]

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 same external sharing practices described on page 15 of the EINSTEIN 2 PIA apply to the proof of concept; Michigan will be granted access to its own network flow records and

[9] EINSTEIN 2 PIA at 12-13.
[10] EINSTEIN 2 PIA at 14.
[11] EINSTEIN 2 PIA at 15.

will be able to run analysis and generate reports to accommodate its own network security interests. No other organization, other than Michigan and US-CERT, will be permitted to see Michigan's network flow records, and Michigan will also not be permitted access to the network flow records of other EINSTEIN 1 participants.

Michigan and the federal executive agencies using US-CERT may be provided trend and summary information that is aggregated from the network flow records of this proof of concept and the network flow records other EINSTEIN 1-participating government agencies. The limited nature of the network flow records and the limited information included in the high-level reports about malicious computer network activities are the same in the proof of concept as the protections described on page 16 of the EINSTEIN 2 PIA – the only distinction being that the proof of concept will only involve network flow records through EINSTEIN 1 system, not the additional network traffic data that is part of EINSTEIN 2 coordination.

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.

This PIA along with the existing PIAs for EINSTEIN 1 and EINSTEIN 2 explain what information is collected and how that information is used. Just as with EINSTEIN 1 and 2, a SORN (system of records notice – a notice requirement of the Privacy Act of 1974) is not required because this proof of concept will not retrieve information by a personal identifier.

In the DHS-Michigan Memorandum of Agreement, Michigan certified that its log-on consent banners or notices; terms-of-use policies or user agreements; computer training programs; or any other mechanisms used to notify users of Michigan government networks that Michigan routinely monitors and may intercept, search or seize communications or data transiting or stored on Michigan information systems, and that any communications or data transiting or stored on Michigan information systems may be disclosed or used as permitted by law.

Michigan provides public notice that it uses special software programs for monitoring and auditing network traffic to identify unauthorized attempts to upload or change information or otherwise to cause damage to their government computer system, and that it uses industry-standard software tools to control access to specific applications and services and protect data that is transmitted electronically between users and Michigan in order to ensure that its users are aware that they monitor and use security software to identify malicious uses of their networks. This notice is available on the Michigan.gov website:

http://www.michigan.gov/som/0,1607,7-192-26916-2301--,00.html

The information contained in network flow records is the basic information involved in any network computer-to-computer communication. It is technically possible but not feasible for the average Internet user to communicate without permitting network flow records to be transmitted to Michigan's computers. As a result, the decision to communicate electronically with Michigan during this proof of concept is essentially a decision to provide network flow records to Michigan.

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 proof of concept does not provide any specific mechanisms for access, redress, or correction. The network flow records used in the proof of concept are generated from exact copies of computer network traffic and only describes minimal amount of information about communications between computers and US-CERT will not add any additional information about individuals associated with those computers including personally identifiable information. As a result, there is minimal amount of information about which to seek access, redress, or correction.

As discussed in the previous section, Michigan has certified that users of covered Michigan government networks receive notice of and consent to the monitoring of communications transiting such networks.

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.

The proof of concept will use the same access and security protections as the current EINSTEIN engagements. As described on page 21 of the EINSTEIN 2 PIA, access to the network flow records in EINSTEIN is strictly limited to trained US-CERT personnel who are governed by the US-CERT standard operating procedures. US-CERT contractors will have access to the network flow records and are subject to the same training, auditing, and oversight that governs the federal employees assigned to the US-CERT.

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 proof of concept will use the same EINSTEIN 1 technology as is currently in use by US-CERT.

Responsible Official

Randall Vickers

Acting Director, US-CERT(888) 282-0870

Department of Homeland Security

Approval Signature

APPROVAL SIGNATURE

Original on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix: Sample Flow Record

The following example of a flow record appears on Page 7-8 of the EINSTEIN 2 PIA:

```
127.0.0.1|192.168.0.20|52119|25|6|10|600|S|2008/04/28T00:02:47.958|44.9
85|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 Flow Record:

- 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