Computer Network Security & Privacy Protection

February 19, 2010

Overview

The Nation's electronic information infrastructure is vital to the functioning of the Government as well as maintaining the Nation's economy and national security. This infrastructure, however, is under perpetual attack by a variety of sources, from novice hackers to sophisticated groups that seek to gain or deny access to, disrupt, degrade, or destroy the systems and the data contained therein. These threats will likely expand over time as more of our critical infrastructure is connected to the Internet, and malicious cyber activity grows in volume and becomes more sophisticated and targeted, creating ever greater potential for more severe consequences.

Leading the protection and defense of the Federal Executive Branch civilian networks against cyber threats, and coordinating response to cyber threats and vulnerabilities, falls within the mission responsibilities of the Department of Homeland Security (DHS).[1] The threat is constantly evolving, requiring DHS to continually evaluate its capabilities and supporting technology. In line with its mission, the Department is upgrading its cybersecurity capabilities— using both proven and emerging technologies—to secure and defend against threats from cyberspace. It is particularly important in this regard to defeat attacks from high-level threat actors who can potentially damage, cripple, exploit, and leverage Federal Executive Branch civilian networks and other critical national systems. While executing this mission, DHS takes the protection of privacy and civil liberties seriously, as discussed in greater detail below.

The use of advanced technologies helps DHS achieve its primary objective, to improve the security of Federal Executive Branch civilian networks. To accomplish this enormous task, the functions or operations of cybersecurity require the use of multiple disciplines. The Department requires close cooperation among network operations as well as sharing cybersecurity information, as appropriate, among the intelligence, communications, counterintelligence, and law enforcement communities. Moreover, each agency that operates a network uses its inherent capabilities and authorities and retains primary responsibility for securing and defending its own networks and critical information infrastructure. However, DHS will assist by performing data and report analysis to reduce cyber threats and vulnerabilities, disseminating cyber alert and warning information to promote protection against cyber threats, coordinating with partners and

[1] Comprehensive National Cybersecurity Initiative, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (January 8, 2008) and the Federal Information Security Management Act of 2002 (FISMA). This is covered in more detail below.

customers to attain shared cyber situational awareness, and providing response and recovery support.

The governing statutory authorities for this mission are the Homeland Security Act of 2002 (HSA) and the Federal Information Security Management Act of 2002 (FISMA). Directives from the President further refine the Department's role. Homeland Security Presidential Directive (HSPD) 5 establishes DHS's incident management responsibilities in the event of a terrorist attack or presidential major disaster or emergency declaration, while HSPD 7 requires DHS to maintain an organization to serve as the focal point for cybersecurity coordination among Federal departments and agencies, State and local governments, the private sector, academia, and international organizations. DHS established the United States Computer Emergency Readiness Team (US-CERT) in 2003, which is identified by the Office of Management and Budget (OMB) to serve under FISMA as the Federal information security incident center to:

- Provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;
- Compile and analyze data about incidents that threaten information security; and
- Inform operators of agency information systems about current and potential information security threats and vulnerabilities.

National Security Presidential Directive (NSPD) 54/ HSPD 23, which formalized the Comprehensive National Cybersecurity Initiative (CNCI), authorizes DHS, together with OMB, to establish minimum operational standards for Federal Executive Branch civilian networks so that US-CERT can direct the operation and defense of government connections to the Internet.

NSPD 54/HSPD 23, along with critical infrastructure protection authorities under the HSA, empower DHS to lead and coordinate the national effort in the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure availability, integrity, authenticity, confidentiality, and non-repudiation is maintained across cyberspace. The Department's intrusion detection and intrusion prevention efforts, called EINSTEIN and described in more detail below, are being implemented pursuant to DHS's role and authorities described above.

With respect to privacy, NSPD 54/HSPD 23 specifically enumerates that CNCI program initiatives, including EINSTEIN, will be implemented in a manner that ensures that the privacy rights and other legal rights of Americans are protected. Since the Directive identified the Secretary of Homeland Security as the lead for the national effort to protect, defend, and reduce vulnerabilities of Federal Executive Branch civilian networks,

the Department's statutorily mandated privacy provisions apply to each of DHS's CNCI activities.[2]

Computer Network Security Activities

Established in 2003 and serving as the Federal information security incident center under FISMA,[3] US-CERT's mission includes: analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. Operating a 24/7/365 operations center, the US-CERT is the lead entity in the national effort to provide situational awareness and timely and effective technical assistance to operators of Federal Executive Branch civilian information systems regarding information security incidents. This includes providing guidance on detecting and handling information security incidents; compiling and analyzing information about incidents that threaten information security; and informing operators of Department and Agency information systems about current and potential information security threats and vulnerabilities. Additionally, US-CERT provides consolidated intrusion detection, incident analysis, and cyber response capabilities to protect Federal Executive Branch civilian agencies' external access points.

To achieve these mission capabilities, DHS must develop and use new and emerging technologies. The Department uses EINSTEIN, which is part of a "system-of-systems" approach that encompasses the people, processes, and technologies needed to create a front line of defense and to grow the Nation's future capabilities and capacities necessary to respond to new and emerging threats. The first iteration of the EINSTEIN system was developed in 2003. EINSTEIN 1 is a network flow monitor, designed to identify malicious activity through changes in the trends in network traffic. In 2008, DHS incorporated the capabilities of EINSTEIN 1 into a follow-on version that includes a computer network security intrusion detection system (IDS) and that version is called EINSTEIN 2. DHS is currently deploying EINSTEIN 2 to Federal Executive Branch civilian Departments and Agencies.

DHS is installing EINSTEIN capabilities on Federal Executive Branch civilian networks in distinct but interconnected steps. First, consolidation of and applying appropriate protection for external connections is an essential first step in creating an efficient and manageable front line of defense for Federal executive branch civilian networks. This initial phase requires that the Government understand how civilian Departments and Agencies configure their external connections—or Internet access points—and improve security for those connections. The Department is accomplishing this through the CNCI's Trusted Internet Connection (TIC) initiative.

Next, as Departments and Agencies consolidate their Internet connections, DHS is deploying EINSTEIN 2 to TIC locations to monitor incoming and outgoing traffic for

[2] The DHS Privacy Office serves as the steward of Section 222 of the Homeland Security Act, the Privacy Act of 1974, the Freedom of Information Act, the E-Government Act of 2002 and the numerous laws, Executive Orders, court decisions and DHS policies that protect the collection, use, and disclosure of personal and Departmental information.

[3] *See* OMB Memorandum, M-06-19, http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf

malicious activity directed toward the Federal Executive Branch's civilian unclassified computer networks and systems. EINSTEIN 2 allows DHS to more effectively identify malicious cyber activity across Federal Executive Branch civilian networks, improving situational awareness and cybersecurity support to Departments and Agencies.

In addition, DHS is in the concept development and testing stage for an intrusion prevention system. Once this testing phase is over, DHS will identify the best equipment and procedures to support the next stage of the EINSTEIN system, EINSTEIN 3. When fully developed, EINSTEIN 3 will be deployed to protect Federal Executive Branch civilian networks and systems. DHS is still developing its intrusion prevention approach with help from the private sector, the National Security Agency (NSA), and a wide range of other Federal partners. Intrusion prevention systems, in general, are designed to detect and defeat malicious cyber activity prior to entry into systems or networks. The goals of the EINSTEIN system are to provide the government with an early warning system, improved situational awareness of intrusion threats to Federal Executive Branch civilian networks, near real-time identification of malicious activity, and prevention of that malicious activity. The eventual addition of the EINSTEIN 3 capability will provide DHS with the ability to automatically detect malicious activity and disable attempted intrusions before harm is done. The EINSTEIN 3 capability to prevent cyber intrusions will be critical to securing and defending Federal Executive Branch civilian networks and systems.

While all of these activities are happening simultaneously, DHS must also focus on the foundation of network defense – the human component. The Department's cybersecurity workforce is a critical element in its ability to effectively secure cyber systems against the continually evolving cyber threat. For this reason, the Department is developing plans with interagency partners to ensure the availability of an abundant, qualified cyber workforce with the knowledge, skills, and operational know-how to solve complex cybersecurity problems.

As has been underscored by Secretary Napolitano, securing the Nation's cyber networks also requires active dialogue and collaboration between the public and private sectors. The need for private industry to become more involved in developing comprehensive, game-changing, innovative solutions that improve and expand upon our current capabilities to protect, detect, and respond to cyber incidents cannot be overemphasized. DHS is working with industry to find technical, end-to-end solutions that will help protect the Federal Executive Branch's civilian networks, and facilitate cybersecurity improvements affecting the private sector. All of these efforts are building a greater national capacity and capability in cybersecurity.

Deploying the EINSTEIN 2 Intrusion Detection System

All Federal Executive Branch civilian agencies are required to participate in the use of the EINSTEIN 2 intrusion detection system, in accordance with the OMB November 20, 2007, Memorandum M-08-05, Implementation of Trusted Internet Connections. EINSTEIN 2 is a commercial off-the-shelf intrusion detection system. It only monitors

Internet and network traffic originating from, or intended for, Federal Executive Branch civilian government networks. It does not monitor traffic on internal Agency networks nor does it monitor commercial or private traffic traversing the public Internet. As emphasized in the EINSTEIN 2 Privacy Impact Assessment (PIA), "E[INSTEIN] 2 passively observes network traffic to and from participating Federal executive agencies' networks."[4]

Such traffic flows to an EINSTEIN sensor either through an authorized Networx Managed Trusted Internet Protocol Service (MTIPS) Internet Service Provider (ISP) TIC location or a TIC location run by an authorized Federal Executive Branch civilian Department or Agency.[5] Mechanisms are in place under either deployment option to ensure that only data traveling to and from Federal Executive Branch civilian networks is routed through EINSTEIN. Both options require the relevant Department or Agency to identify a set range of Internet Protocol (IP) addresses that are used in its network. The Department or Agency will work with its ISP to ensure that only data addressed to or from that Federal network is routed through to the EINSTEIN system.

Managed Trusted Internet Protocol Service

With respect to a Department or Agency that contracts with a Networx ISP for MTIPS, the contract contains a provision requiring the ISP to ensure that only data routed to or from the Department or Agency's IP addresses are sent to the EINSTEIN system. Specifically, the ISP's General Services Administration (GSA) Networx MTIPS Statement of Work (SoW) provides that:

> "…traffic collection and distribution supports the transport of Government-only IP traffic between Agency Enterprise WANs and TIC Portals…. The TIC Portal…monitoring and management systems shall be dedicated to the management and monitoring of the subscribing Agencies hosted by the contractor's portal and shall be isolated from commercial customers."[6]

The ISP further confirms its responsibility to isolate government traffic from that of its commercial customers through a Memorandum of Agreement (MOA) executed with DHS, which references the SoW provisions. A Department or Agency that is using Networx MTIPS also has an MOA with DHS. Pursuant to this MOA, the Department or Agency is responsible for ensuring, in conjunction with the MTIPS provider, that only Department or Agency IP traffic is routed through the EINSTEIN sensor.

Trusted Internet Connection

Similar to Departments and Agencies that utilize Networx MTIPS, those using a TIC will already have a contractual relationship in place with their ISP, usually a Networx ISP. Pursuant to that relationship, the ISP, in its ordinary course of business, will use routing tables to ensure that only traffic intended for the Department or Agency's IP addresses is routed to the Department or Agency's networks. And the Department or Agency remains responsible for ensuring that only traffic intended for, or originating from, that Department or Agency is routed through the EINSTEIN sensor.

---

[4] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_Einstein2.pdf

[5] The following two sections discuss MTIPS and TIC in greater detail.

[6] http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/Managed%20Trusted%20Internet%20Protocol%20Service_REDACTED-Final_R2-z96W_0Z5RDZ-i34K-pR.pdf and http://www.gsa.gov/Portal/gsa/ep/programView.do?pageTypeId=17112&ooid=16100&programPage=%2Fep%2Fprogram%2FgsaDocument.jsp&programId=15914&channelId=-24762

Since EINSTEIN collects network flow information for all traffic traversing a sensor, if, in a rare case the required contractual routing protections fail, in the normal course only network flow information associated with the improperly routed traffic would be collected. This mechanism minimizes the possibility of capturing or releasing Personally Identifiable Information (PII). If improperly routed network traffic matched a pattern of known malicious activity an alert would be triggered. In the event of an alert, and upon further inspection and investigation with the Department or Agency receiving the incorrectly routed traffic, a US-CERT analyst would be able to identify an incorrectly routed traffic error. US-CERT would then work with NCSD's Network Security Deployment and Federal Network Security branches, the relevant Department or Agency, the ISP and, if necessary, the MTIPS vendor, to remedy the routing problem. In the unlikely event that an ISP's routing tables mistakenly assign a government IP address to a commercial client, a routing loop would result. The routing loop would cause errors and break the commercial customer's connection. When the ISP detects the routing loop or the customer reports its broken connections to the ISP, the ISP would correct the error in its ordinary course of business.

EINSTEIN Collection Procedures

As previously noted, individual Federal Executive Branch civilian agencies must monitor their networks and systems and the traffic that flows to and from those systems under authority from FISMA. US-CERT assists those agencies by monitoring the traffic flow in order to provide incident analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. EINSTEIN 2 employs signatures to detect and alert against known computer security threats and vulnerabilities. Signatures are specific patterns of network traffic that detect known specific malicious traffic or activity. The purpose of these signatures is to detect malicious activity directed toward Federal Executive Branch civilian networks.

US-CERT uses indicators of malicious activities to create signatures for inclusion in EINSTEIN 2's intrusion detection capabilities. All signatures are reviewed by the US-CERT in accordance with its signature review process before being employed. Signatures are derived from numerous sources, such as commercially or publicly available computer security information, incidents reported to the US-CERT, information from our Federal partners, and independent in-depth analysis by the US-CERT.

Department and Agency EINSTEIN Deployment and Privacy Protection Requirements

Developing and implementing the technical solutions necessary to secure the Federal Executive Branch civilian networks and systems is complicated and requires sophisticated technology. At the same time, these solutions must ensure the continued protection of civil rights/civil liberties and privacy. DHS, the White House, and all

Federal Executive Branch civilian Departments and Agencies take such protections very seriously.

Accordingly, DHS and its partners have taken decisive steps to incorporate civil liberties and privacy protections as they add, upgrade, and build upon existing defensive cybersecurity capabilities. Each iteration of EINSTEIN incorporates civil liberties and privacy protections into the operating procedures and the architectural engineering development and deployment schedule. In addition, cybersecurity personnel receive specific training on the protection of privacy and other civil rights and civil liberties as they relate to computer network security operations and activities. As an added layer of protection, DHS established an Oversight and Compliance Officer within the Office of the Assistant Secretary for Cybersecurity and Communications. This officer's primary functions are to: monitor the EINSTEIN program; provide specifically tailored privacy cybersecurity training; and to provide information oversight and compliance. DHS's Chief Privacy Officer is part of the development team and conducts privacy impact assessments on aspects of the EINSTEIN system that warrant such review. In this regard, the DHS Chief Privacy Officer is reviewing all components of the EINSTEIN system to determine which elements require a PIA, and will publish as much of the privacy analysis as possible, consistent with security classification.

In addition, the Chief Privacy Officer provides privacy training and oversight to US-CERT personnel and the maintenance personnel of the EINSTEIN system. Furthermore, the DHS Office for Civil Rights and Civil Liberties (CRCL) is reviewing the EINSTEIN system; how it is operated by NCSD; and, providing advice to NCSD on how enhanced cybersecurity efforts may be conducted in a manner consistent with civil rights and civil liberties. Finally, US-CERT operates the EINSTEIN system and follows required operational privacy protection procedures that augment the architectural engineering protections.

EINSTEIN Privacy Impact Assessments

The PIAs for EINSTEIN 1 and EINSTEIN 2 are publicly available at www.dhs.gov/privacy. Departments and Agencies are responsible for publishing PIAs when they collect information from the public using technology owned and operated by that Department or Agency. EINSTEIN is a DHS owned and operated system and, as such, the Department has a PIA for the EINSTEIN system published on the DHS Privacy Office website. According to the PIA, the information that is transmitted to or from the Department or Agency is copied and routed through the EINSTEIN 2 intrusion detection sensor. The DHS EINSTEIN 2 PIA informs the public that DHS receives copies of the original network flow data transmitted to or from those Departments or Agencies that participate in the EINSTEIN 2 program and uses commercially available tools to analyze the data for anomalous or malicious activity. Additionally, DHS only retains and reviews data that is associated with known anomalous indicators that triggers an alert on the intrusion detection system.

Individual Department and Agency Requirements and Responsibilities

As part of enrolling in EINSTEIN 2, each Department or Agency is required to certify that it has implemented procedures to provide appropriate notice to its employees that by using government-owned information systems the employees acknowledge and consents to the monitoring, interception, and search of their communications transiting through or stored on those systems. These procedures, which include computer-user agreements, log-on banners, and computer-training programs,[7] ensure that employees are fully informed about the security monitoring in place and that they have no expectation of privacy in their use of these government systems.

Additionally, under OMB Memorandum, M-05-04, Policies for Federal Agency Public Websites (December 17, 2004), Departments and Agencies are required to post their privacy policy information on their websites. This is to inform visitors how they manage and use the information transmitted to their websites and how it may be used and shared with law enforcement.

Information Handling

Department & Agency Specialized Handling Requirements

Other Federal Departments or Agencies can better speak about what they do to protect information transmitted to or from their systems. However, Federal Executive Branch civilian Departments and Agencies using the EINSTEIN services must notify US-CERT in writing of any special information handling or security requirements arising from law applicable to their Department or Agency information. They must also coordinate with US-CERT's points of contact to institute appropriate safeguards for data that will be monitored by the EINSTEIN 2 intrusion detection system.

Retention of PII

Currently, US-CERT is working with the DHS Under Secretary for Management's Senior Records Officer to have the National Archive and Records Administration approve a general records schedule for the information handled by the EINSTEIN 2 system. Moreover, the Department is proposing to retain this information for the shortest amount of time that is operationally relevant.

As for the retention of PII[8], US-CERT has procedures in place to ensure that PII will be deleted in a timely fashion, to the maximum extent possible. Information captured in a computer network security vulnerability alert is initially examined to determine if there is any information present that could potentially contain PII. US-CERT minimizes PII information to only what is needed for analysis. If a determination is made that retention of PII is needed, then further analysis is required. If it is then found that the computer

[7] Memorandum, Department of Justice, Office of Legal Counsel, Subject: 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 (December 16, 2008). http://www.usdoj.gov/olc/2009/e2-issues.pdf

[8] OMB Memorandum M-07-16,http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf; OMB Memorandum, M-06-19,http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf; OMB Memorandum, M-03-22, http://www.whitehouse.gov/omb/memoranda_m03-22/

network security vulnerability information contains information that either by itself or in combination with other information directly links to an individual, then it is documented that PII has been collected. It must be emphasized that PII will only be included in a computer network security vulnerability product if it is directly necessary to an understanding of the underlying vulnerability threat information. Sharing of that information will be made in strict accordance with the applicable laws and procedures.

System of Record Notice (SORN)

The DHS will continue to comply with the Privacy Act of 1974 and applicable system of records notices for those initiatives under its responsibility. Currently, the US-CERT does not retrieve any information from its databases using any personal identifier. Accordingly, no system of records notice has been required.

Dissemination of Information

US-CERT provides a service that allows each participating Federal Executive Branch civilian Department or Agency to access its own specific EINSTEIN 2 flow records, but not the flow records of other participating Departments. US-CERT shares the processed computer network information collected through EINSTEIN 2, pursuant to executed MOAs, with the specific Agency on whose network the malicious activity was discovered.

Federal Executive Branch civilian Departments and Agencies are also able to obtain access to a secured US-CERT website that contains trend and summary information on computer network security. This information is based in part on EINSTEIN 2 information, but does not contain any PII obtained through EINSTEIN 2 that is not necessary to understand a given security incident. Data received through EINSTEIN is used to provide detection and mitigation strategies to its customers through US-CERT's products. To date, there has not been a product prepared and released by the US-CERT that has contained PII, meaning information that could be specifically identified or linked to a specific individual.

The US-CERT is a computer network defense and security organization that is responsible for increasing the security of Federal Executive Branch civilian networks, not conducting investigations or obtaining attribution for a particular event. Computer network security is, however, accomplished using multiple disciplines to secure the Federal network, with some support provided by law enforcement, intelligence, and other agencies. These other agencies are notified when a computer network event occurs that falls within their responsibility. US-CERT works with that entity when an event has occurred and provides them with contact information so they can coordinate directly with the affected participating Federal Department or Agency.

Oversight & Compliance

The DHS Privacy Office is the first statutorily required Privacy Office at any Federal Department or Agency; its mission is to minimize the impact on the individual's privacy, particularly the individual's personal information, while achieving the mission of DHS.

The DHS Privacy Office serves as the steward of Section 222 of the HSA, the Privacy Act of 1974, the Freedom of Information Act, the E-Government Act of 2002 and the numerous laws, Executive Orders, court decisions and Department policies that protect the collection, use, and disclosure of personal and Departmental information.
In this role, the DHS Privacy Office has authority to investigate and have access to all materials to make such investigations and reports, as it deems necessary, to include the Department's cybersecurity efforts.[9]

The Office of Cybersecurity and Communications (CS&C) established a formal Oversight & Compliance Officer, formally a senior policy strategist, to oversee all information handling requirements, policies, and procedures, including those, which protect privacy, and civil rights and civil liberties. This official fulfills this responsibility by auditing and inspecting the activities of the EINSTEIN program —as well as other information practices—to ensure functions are executed in conformance with legal and policy objectives. The CS&C official is also available to consult with DHS components as a subject matter expert in planning and executing cybersecurity activities that touch upon privacy and information handling. Moreover, the official is also the a liaison to the Department's Chief Privacy Office and DHS CR/CL, thus ensuring that privacy, civil rights, and civil liberty concerns are interwoven into all aspects of cybersecurity planning and execution.

Privacy Guidelines and Training Materials

All US-CERT personnel undergo annual privacy protection training from the DHS Privacy Office. In addition, all US-CERT personnel receive specialized training on "Computer Network Security Oversight & Compliance." The specialized training covers the information handling procedures and the limitations of the computer security role, emphasizing that this role is to secure systems and networks and not to investigate events or individuals. The training concludes with lessons learned analyses and situational training exercises.

Role of the National Security Agency

The NSA assists DHS by providing technical assistance where necessary. In addition to NSA's assistance, DHS gained insights from a wide range of Federal and private sector partners to inform the architecture of EINSTEIN both present and future. To be clear, the Department has a strong and positive relationship with the NSA, and the NSA regularly provides information assurance, technical assistance, vulnerability and threat information to other government agencies, a responsibility which is recognized in several Federal statutes including FISMA.

Private Sector Participation

The Department understands that securing the Nation's cyber networks requires active dialogue, collaboration, and teaming between the public and private sectors and is

[9] 6 USC § 142

committed to this task. DHS has implemented a robust public-private partnership that has made tremendous progress toward securing the Nation's critical infrastructure and key resources (CIKR). DHS created the National Infrastructure Protection Plan (NIPP) and related Sector-Specific Plans (SSPs) to achieve a safer, more secure and more resilient America. The NIPP requires that the SSPs be implemented across all CIKR sectors.

DHS realizes that it is essential for private industry to become more involved in developing comprehensive, game-changing, innovative solutions that improve and expand upon DHS' current capabilities to protect, detect, and respond to cyber incidents. In January 2009, CS&C hosted an Industry Day to further open the dialog between public and private sector technology providers.

As a follow up to Industry Day, DHS released a request for information (RFI) that private sector information on prospective technical, end-to-end solutions for protecting Federal Executive Branch civilian networks, which includes capabilities that could be applied as part of future developments. This effort will help develop innovative technology solutions to address future cyber challenges while strengthening the public-private partnerships that are critical to cybersecurity.

As previously mentioned, DHS also participates in the efforts of the MTIPS delivered via the ISP's General Services Administration Networx contract.

Future Program Development

The current developmental phase of the EINSTEIN program is an exercise to evaluate and demonstrate potential future capabilities. The exercise is intended to inform DHS on an architectural and procedural solution to build upon EINSTEIN 2 by adding intrusion prevention capabilities.

The exercise will demonstrate the ability to isolate and route specified Federal Executive Branch civilian network traffic flowing through the vendor's network to DHS equipment and the ability to complete delivery of Department and Agency network traffic to its intended destination without adversely impacting operations. The exercise contract will not increase the vendor's access to the traffic that flows to or from the Government.