

March 2010

# INFORMATION SECURITY

## Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies



GAO

Accountability \* Integrity \* Reliability



Highlights of [GAO-10-237](#), a report to congressional requesters

## Why GAO Did This Study

To reduce the threat to federal systems and operations posed by cyber attacks on the United States, the Office of Management and Budget (OMB) launched, in November 2007, the Trusted Internet Connections (TIC) initiative, and later, in 2008, the Department of Homeland Security's (DHS) National Cybersecurity Protection System (NCPS), operationally known as Einstein, became mandatory for federal agencies as part of TIC. For each of these initiatives, GAO was asked to (1) identify their goals, objectives, and requirements; (2) determine the status of actions federal agencies have taken, or plan to take, to implement the initiatives; and (3) identify any benefits, challenges, and lessons learned. To do this, GAO reviewed plans, reports, and other documents at 23 major executive branch agencies, interviewed officials, and reviewed OMB and DHS guidance.

## What GAO Recommends

GAO is making recommendations to OMB to promptly communicate the number of approved connections for agencies, and to DHS aimed at improving communication and performance measures. OMB concurred with GAO's findings, conclusions, and recommendations. DHS concurred with GAO's recommendations and also provided technical comments.

View [GAO-10-237](#) or [key components](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or [wilshusen@gao.gov](mailto:wilshusen@gao.gov).

## INFORMATION SECURITY

### Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies

#### What GAO Found

The goals of TIC are to secure federal agencies' external network connections, including Internet connections, and improve the government's incident response capability by reducing the number of agencies' external network connections and implementing security controls over the connections that remain. In implementing TIC, agencies could either provide their own access points by becoming an access provider or seek service from these providers or an approved vendor. To achieve the initiative's goals, agencies were required to

- inventory external connections,
- establish a target number of TIC access points,
- develop and implement plans to reduce their connections,
- implement security capabilities (if they chose to be an access provider) addressing such issues as encryption and physical security, and
- demonstrate to DHS the consolidation of connections and compliance with the security capabilities (if they chose to be an access provider).

As of September 2009, none of the 23 agencies had met all of the requirements of the TIC initiative. Although most agencies reported that they have made progress toward reducing their external connections and implementing critical security capabilities, most agencies have also experienced delays in their implementation efforts. For example, the 16 agencies that chose to become access providers reported that they had reduced their number of external connections from 3,286 to approximately 1,753. Further, agencies have not demonstrated that they have fully implemented the required security capabilities. Throughout their reduction efforts, agencies have experienced benefits, such as improved security and network management. However, they have been challenged in implementing TIC because OMB did not promptly communicate the number of access points for which they had been approved and DHS did not always respond to agency queries on security capabilities in a timely manner. Agencies' experiences with implementing TIC offered OMB and DHS lessons learned, such as the need to define program requirements before establishing deadlines and the usefulness of sponsoring collaborative meetings for agencies' implementation efforts.

Einstein is intended to provide DHS with an increased awareness of activity, including possible security incidents, on federal networks by providing intrusion detection capabilities that allow DHS to monitor and analyze agencies' incoming and outgoing Internet traffic. As of September 2009, fewer than half of the 23 agencies had executed the required agreements with DHS, and Einstein 2 had been deployed to 6 agencies. Agencies that participated in Einstein 1 improved identification of incidents and mitigation of attacks, but DHS will continue to be challenged in understanding whether the initiative is meeting all of its objectives because it lacks performance measures that address how agencies respond to alerts.

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Background	3
	Agencies Have Made Progress toward Consolidating and Reducing Connections, but Inconsistent Communication from OMB and DHS Has Led to Challenges	10
	DHS Has Deployed Einstein to Six Agencies, but Faces Challenges with Meeting Program Goals	23
	Conclusions	29
	Recommendations for Executive Action	30
	Agency Comments	31
<b>Appendix I</b>	<b>Objectives, Scope, and Methodology</b>	<b>33</b>
<b>Appendix II</b>	<b>GAO Contact and Staff Acknowledgments</b>	<b>35</b>
<b>Tables</b>		
	Table 1: Reported Status of Consolidation by 19 Agencies	14
	Table 2: Number of Critical Security Capabilities Reported as Implemented by Access Provider Agencies	16
<b>Figures</b>		
	Figure 1: Interaction of TIC and Einstein	9
	Figure 2: Comparison of Reported Consolidation by 16 Access Provider Agencies	15

---

---

## Abbreviations

DHS	Department of Homeland Security
GSA	General Services Administration
NCPS	National Cybersecurity Protection System
OMB	Office of Management and Budget
TIC	Trusted Internet Connections
US-CERT	United States Computer Emergency Readiness Team

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office  
Washington, DC 20548

March 12, 2010

The Honorable Joseph I. Lieberman  
Chairman  
The Honorable Susan M. Collins  
Ranking Member  
Committee on Homeland Security and Governmental Affairs  
United States Senate

The Honorable Thomas R. Carper  
Chairman  
Subcommittee on Federal Financial Management, Government  
Information, Federal Services, and International Security  
Committee on Homeland Security and Governmental Affairs  
United States Senate

Pervasive and sustained cyber attacks against the United States continue to pose a potentially devastating impact on federal systems and operations. The need for a vigilant approach to information security is demonstrated by a dramatic increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology. As recently as July 2009, press accounts reported that a widespread and coordinated attack over the course of several days targeted Web sites operated by major government agencies, including the Departments of Homeland Security and Defense, the Federal Aviation Administration, and the Federal Trade Commission, causing disruptions to the public availability of government information. In addition, the Director of National Intelligence testified in February 2009 that foreign nations and criminals had targeted government and private-sector networks to gain a competitive advantage or potentially disrupt or destroy them, and that terrorist groups had expressed a desire to use cyber attacks as a means to target the United States.<sup>1</sup> Such attacks and threats highlight the importance of developing a concerted response to safeguard federal information systems.

---

<sup>1</sup>Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence*, statement before the Senate Select Committee on Intelligence (Feb. 12, 2009).

---

To improve the effectiveness of information security across the federal government, in November 2007, the Office of Management and Budget (OMB) announced the Trusted Internet Connections (TIC) initiative, and in 2003 the Department of Homeland Security (DHS) established the Einstein program, recently incorporated into the National Cybersecurity Protection System (NCPS). TIC is intended to improve security by reducing and consolidating external network connections and by providing centralized monitoring at a select group of access providers, while Einstein is an intrusion detection system that provides an automated process for DHS to analyze computer network traffic information from agencies. In January 2008, these programs were incorporated into the Comprehensive National Cybersecurity Initiative.<sup>2</sup>

At your request, we evaluated key elements of the implementation of TIC and Einstein at federal agencies. For each of these initiatives, we (1) identified the goals, objectives, and requirements for the initiatives; (2) determined the status of the actions federal agencies have taken, or plan to take, to implement the initiatives; and (3) identified the benefits, challenges, and lessons learned in implementing the initiatives.

To accomplish our objectives, we examined OMB memorandums and DHS guidance in order to identify program requirements, which we confirmed through interviews with OMB and DHS officials. We obtained and analyzed plans, status reports, and other documents and interviewed officials from 23 of the 24 federal agencies listed in the Chief Financial Officers Act.<sup>3</sup> The Department of Defense was not included in our review because it was not required to implement TIC or Einstein. The initiatives include additional agencies which were not included in our review.

---

<sup>2</sup>The Comprehensive National Cybersecurity Initiative consists of 12 projects intended to improve DHS's and other federal agencies' efforts to safeguard federal executive branch government information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats against the federal government's networks.

<sup>3</sup>The 24 agencies subject to the act are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

---

We conducted this performance audit between December 2008 and March 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Further details of our objectives, scope, and methodology are included in appendix I.

---

## Background

As computer technology has advanced, federal agencies have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions, deliver services to the public, and account for their resources without these cyber assets. Information security is thus especially important for federal agencies to ensure the confidentiality, integrity, and availability of their systems and data. Conversely, ineffective information security controls can result in significant risk to a broad array of government operations and assets, as the following examples illustrate:

- Computer resources could be used for unauthorized purposes or to launch attacks on other computer systems.
- Sensitive information, such as personally identifiable information, intellectual property, and proprietary business information could be inappropriately disclosed, browsed, or copied for purposes of identity theft, espionage, or other types of crime.
- Critical operations, such as those supporting critical infrastructure, national defense, and emergency services, could be disrupted.
- Data could be added, modified, or deleted for purposes of fraud, subterfuge, or disruption.

Due to the growing cyber-based threats to federal systems and critical infrastructure, the persistent nature of information security vulnerabilities, and the associated risks, we continue to designate information security as a governmentwide high-risk issue in our most recent biennial report to

---

Congress,<sup>4</sup> a designation we have made in each report since 1997. In July 2009, we reported<sup>5</sup> that almost all 24 major federal agencies had weaknesses in information security controls and that an underlying reason for these weaknesses is that agencies have not fully implemented their information security programs as required under the Federal Information Security Management Act.<sup>6</sup> As a result, federal systems and sensitive information are at increased risk of unauthorized access and disclosure, modification, or destruction, as well as inadvertent or deliberate disruption of system operations and services.

We have previously reported that federal agencies have experienced security breaches in their networks, potentially allowing sensitive information to be compromised, and systems, operations, and services to be disrupted. These examples illustrate that a broad array of federal information and critical infrastructures are at risk:<sup>7</sup>

- The Department of State experienced a breach on its unclassified network, which daily processes about 750,000 e-mails and instant messages from more than 40,000 employees and contractors at 100 domestic and 260 overseas locations.
- The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as “Slammer” infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours.
- Officials at the Department of Commerce’s Bureau of Industry and Security discovered a security breach in July 2006. In investigating this incident, officials were able to review firewall logs for an 8-month period prior to the initial detection of the incident, but were unable to clearly define the amount of time that perpetrators were inside its computers, or find any evidence to show that data was lost as a result.

---

<sup>4</sup>GAO, *High-Risk Series: An Update*, [GAO-09-271](#) (Washington, D.C.: January 2009).

<sup>5</sup>GAO, *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses*, [GAO-09-546](#) (Washington, D.C.: July 17, 2009).

<sup>6</sup>The Federal Information Security Management Act was enacted as title III, E-Government Act of 2002, Pub L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

<sup>7</sup>GAO, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, [GAO-08-571T](#) (Washington, D.C.: Mar. 12, 2008).



---

Because the threats have persisted and grown, in January 2008 the President issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23, establishing the Comprehensive National Cybersecurity Initiative,<sup>8</sup> a set of projects with the objective of safeguarding federal executive branch government information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats against the federal government's networks. Under the initiative, DHS is to lead several projects to better secure civilian federal government networks, while other agencies, including OMB, the Department of Defense, the Office of the Director of National Intelligence, and other agencies have key roles in other projects, including monitoring military systems and classified networks, overseeing intelligence community systems and networks, and spearheading advanced technology research and development. The initiative's 12 projects can be grouped into three focus areas:

- *Establishing front lines of defense.* This focus area includes initiatives intended to protect the perimeter of federal networks, such as consolidating connections and deploying intrusion detection and prevention systems.
- *Defend against full spectrum of threats.* This focus area includes activities intended to protect national security and intelligence-related information and systems across the federal government.
- *Shape the future environment.* The initiatives in this area are focused on expansion of cybersecurity education and research and development efforts for future technologies and cybersecurity strategies.

Two primary initiatives under the establishing front lines of defense focus area are TIC and Einstein.

## Trusted Internet Connections

In November 2007, OMB announced the TIC initiative.<sup>9</sup> Directed by OMB with assistance from DHS, this effort is intended to improve the federal government's security posture and incident response capability by

---

<sup>8</sup>GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338 (Washington, D.C.: Feb. 1, 2010).

<sup>9</sup>OMB, *Implementation of Trusted Internet Connections (TIC)*, M-08-05 (Washington, D.C.: Nov. 20, 2007).

---

reducing and consolidating external network connections, including Internet connections, currently in use by the government, and by centrally monitoring the traffic passing through these connections for potentially malicious activity. All federal agencies in the executive branch, except for the Department of Defense, are required to implement the initiative. Although the initiative is intended to secure connections to the Internet, other external connections to potentially unsecured systems must also be routed through an approved TIC access point,<sup>10</sup> even if they do not pass through the Internet.<sup>11</sup>

Agencies may implement TIC by serving as their own access provider or by obtaining services from another source. Agencies may choose one of four service options:

- *Single service*: The agency provides services to its own bureaus and components only.
- *Multi-service*: The agency provides services to its own bureaus and components as well as to other agencies.
- *Seeking service*: The agency obtains services from a multi-service agency or through the Networx program. This program, managed by the General Services Administration (GSA), provides an acquisition vehicle for agencies to procure telecommunication, network, wireless, and information technology security services, including TIC services, from among multiple vendors.
- *Hybrid*: The agency both provides services to its own bureaus and components and obtains additional services from a Networx provider.

Of the 23 agencies in our review, 16 have chosen to be a TIC access provider: specifically, 12 have chosen the single service option, 1 chose the multi-service option, and 3 have chosen the hybrid approach. The

---

<sup>10</sup>According to DHS officials, each authorized TIC access point may include one or more external connections.

<sup>11</sup>Examples of connections that are not required to be routed through an approved TIC include (1) dedicated connections to agency remote offices that do not pass through the Internet, (2) connections made using technology that provides a secure communication mechanism for data transmitted across public networks (i.e., virtual private networks), and (3) connections with other agencies where both agencies have implemented TIC.

---

## Einstein

---

remaining seven agencies have chosen to seek service from another access provider.<sup>12</sup>

NCPS, operationally known as Einstein,<sup>13</sup> was created in 2003 by the United States Computer Emergency Readiness Team (US-CERT)<sup>14</sup> in order to aid in its ability to help reduce and prevent computer network vulnerabilities across the federal government. The initial version of Einstein provided an automated process for collecting, correlating, and analyzing agencies' computer network traffic information from sensors installed at their Internet connections. The Einstein sensors collected network flow records<sup>15</sup> at participating agencies, which were then analyzed by US-CERT to detect certain types of malicious activity. It then coordinated with the appropriate agencies to mitigate those threats and vulnerabilities. US-CERT also used the information from the sensors to create analyses of cross-governmental trends, offering departments and agencies an aggregate picture of external threats against the federal government's networks. Participation in the program was initially voluntary for federal agencies.

In 2008, DHS developed the current iteration of Einstein—Einstein 2—which incorporated network intrusion detection technology into the capabilities of the initial version of the system. Einstein 2 monitors for

---

<sup>12</sup>Although OMB originally designated 17 of the 23 agencies in our review as TIC access providers, one of these agencies has since chosen to seek service from another access provider.

<sup>13</sup>According to DHS officials, in December of 2008, the Einstein program was incorporated into NCPS, a larger collection of systems that includes not only the Einstein sensors, but also other systems providing data correlation and analysis.

<sup>14</sup>Established by DHS, the US-CERT serves as a focal point for the government's interaction with federal and nonfederal entities on a 24-hour-a-day, 7-day-a-week basis regarding cyber-related analysis, warning, information sharing, major incident response, and national-level recovery efforts. It is charged with aggregating and disseminating cybersecurity information to improve warning of and response to incidents, increasing coordination of response information, reducing vulnerabilities, and enhancing prevention and protection. In addition, US-CERT collects incident reports from all federal agencies and assists agencies in their incident response efforts.

<sup>15</sup>Network flow records are records of communications made to an organization's IT systems. The records identify the source and destination Internet Protocol addresses used in the communication, the source and destination ports, the time the communication occurred, and the protocol used to communicate.

---

specific predefined signatures<sup>16</sup> of known malicious activity at federal agency Internet connections and alerts US-CERT when specific malicious network activity matching the predetermined signatures is detected. According to US-CERT, the signatures are not typically included in commercially available databases of known attack signatures, but are developed by US-CERT to look for specific malicious activity based on previous analysis. In addition, participation in Einstein became mandatory as part of the TIC initiative.

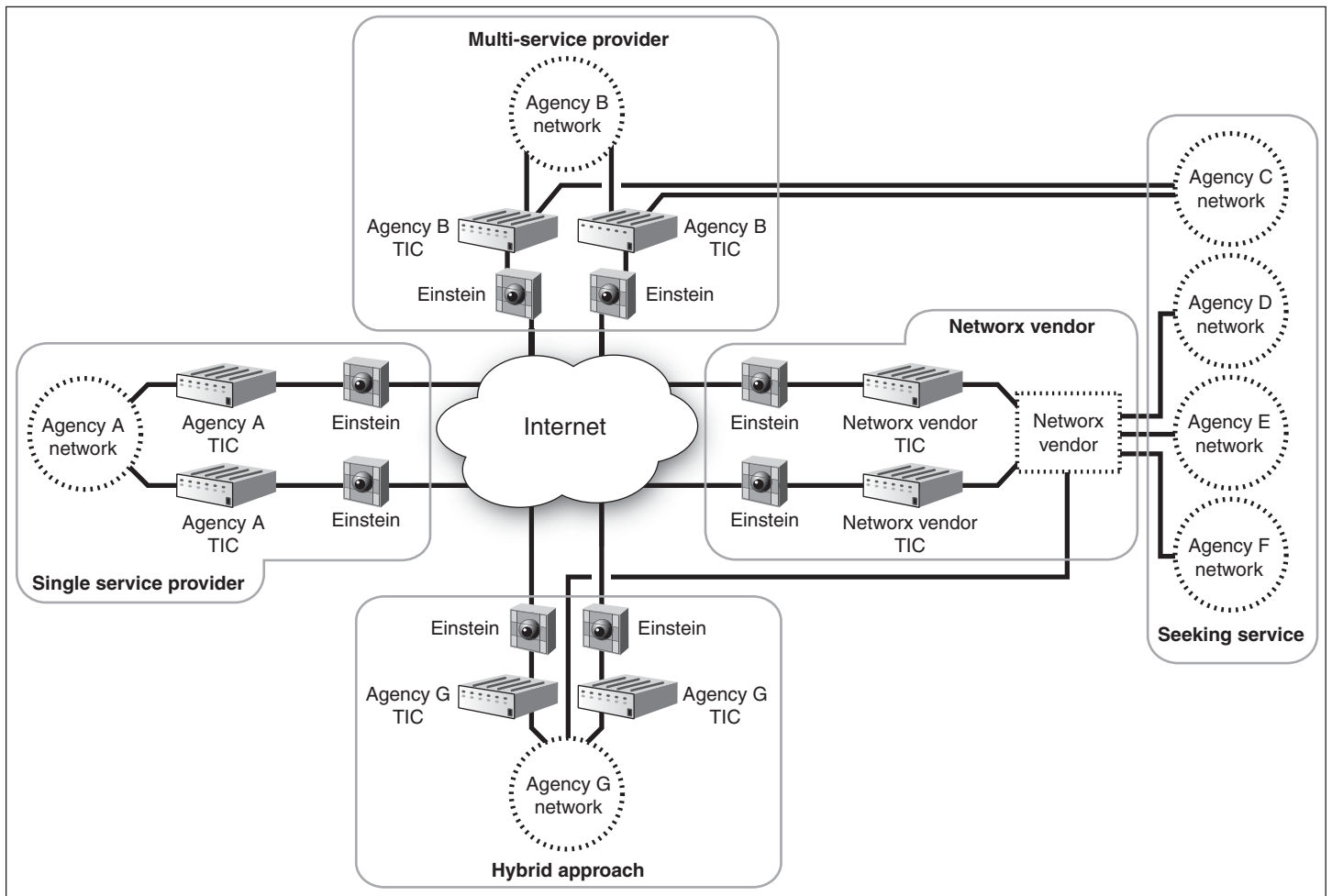
Currently being piloted by DHS, Einstein 3 is intended to be an intrusion prevention system that is to automatically detect and respond appropriately to cyber threats before harm is done. Using signatures developed from critical information about foreign cyber threats as determined by the National Security Agency, the system is to draw on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision making on traffic entering or leaving federal agency networks. It is also intended to support enhanced information sharing by US-CERT with federal agencies by giving DHS the ability to provide agencies with automated alerts of detected network intrusion attempts.

Ultimately, TIC and Einstein are intended to work together to build successive layers of defense mechanisms in the federal government's information technology infrastructures. When Einstein is deployed at a TIC location, it monitors inbound and outbound network traffic. Once TIC is fully implemented across the federal government, all traffic passing between the federal civilian networks and the Internet is to be monitored for malicious activity by US-CERT using Einstein and its supporting processes. Figure 1 illustrates how TIC portals interact with the Einstein sensors and the Internet.

---

<sup>16</sup>Signatures are recognizable, distinguishing patterns associated with cyber attacks, such as a binary string associated with a computer virus or a particular set of keystrokes used to gain unauthorized access to a system.

**Figure 1: Interaction of TIC and Einstein**



Source: GAO analysis based on DHS data.

---

## Agencies Have Made Progress toward Consolidating and Reducing Connections, but Inconsistent Communication from OMB and DHS Has Led to Challenges

OMB and DHS established requirements to meet the initiative's goals of securing agencies' external connections and improving the government's incident response capability. However, as of September 2009, none of the 23 agencies had met all of the requirements. Throughout their efforts, agencies have experienced benefits and challenges as well as learned lessons.

---

## TIC Aims to Improve the Security of Federal Connections to the Internet

The primary goals of the TIC initiative are (1) to secure federal agency external connections using a common set of security controls and (2) to improve the federal government's incident response capability. To achieve these goals, the initiative has the following objectives:

- reduce and consolidate external connections,<sup>17</sup> including connections to the Internet, across the federal government;
- define and maintain baseline security capabilities for TIC access providers; and
- establish a compliance program to monitor agency adherence to TIC policy.

## Agencies Were Required to Develop and Implement Plans to Consolidate and Secure External Connections

To achieve these objectives, agencies were required to:

- **Inventory agency external connections.** Agencies were required to provide their connection inventories to DHS by January 8, 2008.
- **Identify and justify target number of external access points.** Each agency was to submit their target number to DHS by April 15, 2008. They

---

<sup>17</sup>When the initiative was first announced in November 2007, OMB set a target number of 50 connections across the federal government. However, OMB officials have since stated that the target number is no longer applicable and that a new target has not been established.

---

were also required to provide a justification indicating why the requested number of external access points was necessary to support their missions.

- **Develop and implement plans to consolidate external connections.** OMB required agencies to develop and submit initial plans for consolidating their external connections to DHS by January 8, 2008. In addition, agencies were required to update their plans in April 2008. Access provider agencies were required to provide updated plans to DHS in October 2008, and all agencies were required to provide updated plans to DHS in September 2009.

When it announced the initiative in November 2007, OMB required that agencies' initial plans have a target completion date of June 2008 for reducing and consolidating their external connections. OMB later revised its target deadline for implementation of TIC across the federal government to December 2009.

- **Implement security capabilities.** To ensure that each TIC access point would be secure, OMB required<sup>18</sup> agencies that planned to be an access provider to evaluate their ability to meet 74 security capabilities and to report this information to DHS by April 2008. The 74 security capabilities include technical capabilities, such as encryption of Internet traffic and the use of firewalls; capabilities related to availability, such as the presence of an uninterrupted power source; physical access controls; and capabilities that describe how an access provider maintains an acceptable level of service. Of the 74 capabilities, 51 are designated as critical, 14 are designated as important, and 9 are categorized as desired. Of the 51 critical capabilities, 40 are required for both single service and multi-service access providers. The 11 capabilities required only for multi-service access providers address the interaction with external customers, such as service level agreements, communication, and reporting.

OMB provided a template for agencies to report whether they currently met each of the capabilities and to indicate their plans for addressing any critical capabilities they did not meet. Once agencies determined whether to be an access provider or to seek service from another provider, they were required to do one of the following:

---

<sup>18</sup>OMB, *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*, M-08-16 (Washington, D.C.: Apr. 4, 2008).

- 
- Access provider agencies were required to develop plans for implementing any of the critical TIC capabilities that they did not yet have in place. They were required to report on their progress toward implementing the critical capabilities to DHS in October 2008 and September 2009.
  - Agencies that are seeking service from other access providers were not required to implement the critical capabilities; however, they were required to acquire TIC services from a multi-service access provider or a commercial vendor that had met the security capabilities through the Networx contract.
  - **Demonstrate consolidation of connections and implementation of TIC security capabilities.** Access provider agencies, along with Networx vendors that offer TIC services, are required to undergo a TIC Compliance Validation review, in which DHS assesses the degree to which the access provider meets the critical security capabilities and has consolidated its connections to approved TIC access points. If any capabilities are not fully implemented or if further consolidation is required, the access provider is granted Initial Operating Capability status and is required to develop plans to address the shortcomings and to submit the plans to DHS. All access providers are required to be re-assessed periodically to ensure the capabilities are still being met. All access provider agencies were required to schedule the on-site review with DHS by September 25, 2009.

---

### Agencies Have Not Fully Implemented All Requirements of TIC and Progress Has Been Slower Than Planned

None of the 23 agencies has met all of the requirements of the TIC initiative, and most agencies have experienced delays in their plans for reducing and consolidating connections. However, most agencies reported that they have made progress toward reducing and consolidating their external connections and implementing security capabilities. In addition, several access provider agencies have made more progress toward implementing the capabilities than others. The following describes the status of each requirement.

#### All Agencies Submitted Connection Inventories

The 23 agencies in our review reported that they initially identified a total of 3,482 external connections. According to DHS, each agency submitted the required inventories, although four submitted the inventories after the January 2008 deadline. Two agencies told us that they discovered additional connections after submitting the initial inventory.



---

Access Provider Agencies Requested 73 TIC Access Points, but OMB Approved 32

In April 2008, the 16 access provider agencies requested a total of 73 TIC access points. There were a variety of factors that influenced how agencies decided how many access points to request. For example, multiple agencies told us that they chose the number and location of their access points based on the location of existing data centers. Agencies also considered the need for redundant connections, geographic separation between connection sites, the business needs of the agency, and cost factors.

In response to these requests, OMB approved 2 external access points for each access provider agency, a total of 32 TIC access points for the 16 agencies in our review.<sup>19</sup> OMB and DHS established a process for these agencies to request additional access points. As of October 2009, one agency had submitted a request to DHS, and seven other agencies indicated that they had plans to do so.

Progress toward Consolidating Connections Has Been Mixed and Slower than Projected

Progress reported by individual agencies toward meeting their targeted numbers of connections or access points has been mixed, and the reported overall progress toward consolidation has been slower than expected.<sup>20</sup> In submitting their plans, which were due to DHS in October 2008 and September 2009, three agencies reported that they were at their target number of access points and had no further plans to consolidate connections; in addition, one agency did not report the status of its consolidation efforts. Of the remaining 19 agencies, as of September 25, 2009, 6 reported that they had consolidated at least 60 percent of their connections and 9 reported that they had consolidated fewer than 20 percent of their connections. Table 1 shows the consolidation status reported by these 19 agencies as of September 25, 2009.<sup>21</sup>

---

<sup>19</sup>The seven agencies in our review that are seeking service from other providers were not authorized a specific number of access points.

<sup>20</sup>As of September 2009, six access provider agencies were targeting more access points than the number for which they had been approved by OMB.

<sup>21</sup>At the time of our review, one access provider agency had not submitted its September 2009 progress report to DHS; the status of its consolidation effort, reflected in the table, is based on its July 2009 progress report.

---

**Table 1: Reported Status of Consolidation by 19 Agencies**

Agency type	Reported Status of Consolidation				
	Less than 20% <sup>a</sup>	20% to 39%	40% to 59%	60% to 79%	80% to 100%
Access provider	6	1	1	6	0
Seeking service	3	1	1	0	0
<b>Total</b>	<b>9</b>	<b>2</b>	<b>2</b>	<b>6</b>	<b>0</b>

Source: GAO analysis of agency data.

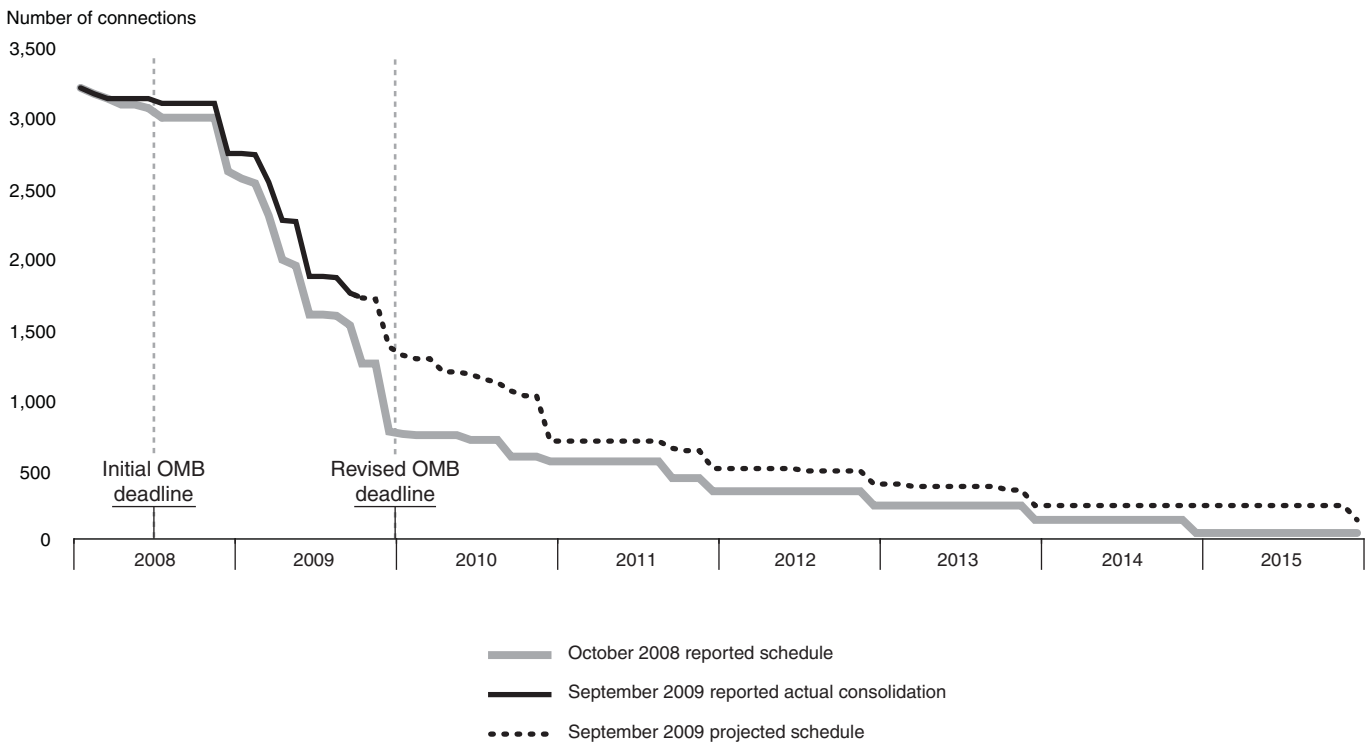
<sup>a</sup>One access provider agency reported that it was less than 20 percent consolidated on September 25, 2009, but that it expected to consolidate to its target of two connections by September 30, 2009.

Overall, the reported progress toward consolidating connections was slower than projected, and agencies delayed their future plans for consolidation. In October 2008, the 16 access provider agencies, which were authorized a total of 32 TIC access points by OMB, projected in their plans of action and milestones that they would consolidate from their initial reported total of 3,286 external connections to a maximum of 1,528 connections by September 2009. However, in their September 2009 plans of action and milestones, these agencies reported that they had consolidated to a maximum of 1,753 connections—225 more than they had planned. In addition, agencies projected in their October 2008 plans that they would have consolidated to a maximum of 764 external connections by OMB’s revised deadline of December 31, 2009. However, in September 2009 they anticipated that they would still have a maximum of 1,374 connections by that date—610 more than originally planned—and had significantly revised their projections for consolidation through November 2010. As agencies continue to consolidate their connections, their future projections for consolidation are likely to be revised further. Figure 2 indicates the estimated overall progress that access provider agencies reported toward reducing connections as of October 2008 and September 2009, their planned future consolidation, and how both their plans and reported progress have changed between October 2008 and September 2009.<sup>22</sup>

---

<sup>22</sup>Seeking service agencies are not included in this figure.

**Figure 2: Comparison of Reported Consolidation by 16 Access Provider Agencies**



Source: GAO estimate based on agency reported data.

Note: In this figure, both of the reported schedules begin at 3,215 connections because one agency reported that it had consolidated 71 connections by January 2008. In addition, at the time of our review, one access provider agency had not submitted its September 2009 progress report to DHS. As a result, the September 2009 projections for this agency were based on an earlier progress report that may not represent the agency's current status or plans.

### Few Agencies Have Reported Implementing All Required Security Capabilities

As of September 2009, only 3 of the 16 access provider agencies have reported implementing all 40 required critical security capabilities.<sup>23</sup> The other 13 agencies have implemented most of the capabilities, but their progress in addressing the remaining capabilities has varied. For example, of those agencies that had not implemented all of the critical capabilities, six reported meeting no additional capabilities between April 2008 and September 2009. Table 2 describes access provider agencies' reported progress toward implementing the capabilities.

<sup>23</sup>The one multi-service access provider agency reported that it had implemented all of the 11 additional critical security capabilities required for multi-service access providers.

**Table 2: Number of Critical Security Capabilities Reported as Implemented by Access Provider Agencies**

Agency	Capabilities reported as implemented in April 2008	Capabilities reported as implemented in September 2009	Change between April 2008 and September 2009
A	27	27	0
B	32	32	0
C	33	34	1
D	33	35	2
E	33	36	3
F	34	38	4
G	35	37	2
H	37	37 <sup>a</sup>	0
I	37	38	1
J	37	39	2
K	38	38	0
L	38	38	0
M	38	40	2
N	39	39	0
O	40	40	N/A
P	40	40	N/A

Source: GAO analysis of agency-provided data.

<sup>a</sup>At the time of our review, agency H had not submitted its September 2009 plan to DHS. This reported number is from an earlier plan that the agency provided to us.

Examples of the capabilities that agencies most frequently reported not having implemented included having secure facilities in place to handle classified information, being able to filter specific types of Internet traffic, and participating in the Einstein program.

Between October 2008 and September 2009, agencies delayed their plans for implementing the critical security capabilities. Of the 13 access provider agencies that had not implemented all of the required capabilities as of September 2009, 6 agencies delayed their expected planned dates for implementing the remaining critical capabilities between approximately 10 months and 3 years. As of September 2009, nine of these agencies were reporting that they expected to complete implementation of the remaining critical security capabilities between September 2009 and December 2010, one expected to complete its efforts in December 2013, and three did not project a date by which they expected to complete implementation.

---

Agencies Have Not Demonstrated Full Compliance with TIC Capabilities or Completed Consolidation Efforts

Agencies have not demonstrated full compliance with TIC capabilities. As of September 2009, DHS had conducted TIC Compliance Validation reviews at 6 of the 16 agencies in our review that are required to undergo a review, and the remaining 10 had been scheduled to be evaluated between October 2009 and May 2010.<sup>24</sup>

The results of the reviews indicated that information that agencies had reported was not always accurate. Specifically, although agencies had reported that certain capabilities were in place, the results for five of the six agencies that completed reviews indicated that several of these capabilities had not been fully implemented. For example, one agency's results showed that it had not fully implemented 10 critical capabilities, including 7 that it had previously reported as complete. In addition, the results for another agency showed that it had a large number of connections that it had not previously reported; the agency originally reported 119 connections, but after the review it identified 403 external connections. As indicated earlier, agencies are required to develop plans to address any shortcomings identified in the review and to submit their plans to DHS.

---

Agencies Experienced Benefits and Lessons Learned in Implementing TIC, but Challenges Remain in Complying with Requirements

While the TIC initiative offers benefits to agencies, such as improved network security, agencies have been challenged in complying with the requirements of the initiative, in part because of shortcomings in communication by OMB and DHS. In addition, agencies' experiences in implementing TIC offers valuable lessons learned for OMB and DHS that may increase the likelihood of the initiative's success.

Benefits in Improved Security and Network Management Are Anticipated

Although agencies are still in the process of implementing TIC, the initiative offers benefits to agencies.

**Improved Network Security.** TIC will improve security at agencies by reducing the number of access points that have to be monitored. Several agencies indicated that consolidating connections and centralizing security monitoring at TIC access points should make it easier to monitor traffic and protect their networks from attacks. In addition, officials from

---

<sup>24</sup>According to DHS officials, only one of the four participating Network vendors had passed a review and could offer TIC services to agencies.

---

---

Agencies Faced Challenges  
with Implementing TIC  
Requirements

another agency stated that the consolidation of external connections had made the agency's network perimeter more secure.

**Improved Network Management.** The initiative has also helped improve agencies' management of their networks. Several agencies stated that implementing TIC by consolidating their external connections is beneficial because it has forced them to gain a greater awareness of their overall network environment. Another agency anticipated that TIC implementation would reduce complexity in its network, making it simpler to manage.

Agencies continue to face challenges in implementing TIC, including implementing the initiative with incomplete information about the number of access points for which they have been approved and about the technical security capabilities. Further, DHS will continue to face challenges in knowing whether the access points are adequately secured.

**Implementing the initiative with incomplete information.** Best practices for program management, established by the Project Management Institute in *The Standard for Program Management*,<sup>25</sup> state that the information that program stakeholders need should be made available in a timely manner throughout the life cycle of a program. In addition, our *Internal Control Management and Evaluation Tool*<sup>26</sup> states that when communicating with other agencies, managers should provide timely information that is relevant to the requester's needs. However, in some circumstances, agencies have been unable to effectively plan for implementing the initiative because OMB did not always consistently communicate the number of TIC access points for which agencies had been approved in a timely manner and DHS did not always promptly respond to agencies' questions about the required security capabilities.

OMB did not consistently inform agencies about the number of TIC access points for which they had been approved until more than a year after it required agencies to submit their requested number. In a memo issued in

---

<sup>25</sup>Project Management Institute, *The Standard for Program Management, Second Edition* (Newton Square, Pa.: 2008).

<sup>26</sup>GAO, *Internal Control Management and Evaluation Tool*, [GAO-01-1008G](#) (Washington, D.C.: August 2001).

---

September 2009,<sup>27</sup> OMB announced that access provider agencies were each allowed two access points, 17 months after its April 2008 deadline for agencies to submit their requested number of trusted connections. However, between April 2008 and September 2009, OMB's communication of the number of access points it had approved for agencies was inconsistent. Specifically,

- Several agencies told us that OMB, or DHS rather than OMB, verbally told them about the number of access points for which they had been approved but did not provide them with written confirmation of the approved number.
- One agency said that it received an e-mail from DHS, as opposed to OMB, stating that its top two to three locations had been approved; however, officials from the agency indicated that the agency was not informed of the exact number of approved access points.
- A few other agencies stated that OMB never informed them of the number of approved access points, either verbally or in writing.

OMB addressed these shortcomings by issuing the memo in September 2009; however, any further inconsistencies in communication by OMB could cause additional challenges for agencies. In the memo, OMB also informed access provider agencies about the process for submitting an evidence-based rationale to DHS to request additional TIC access points. In this process, OMB is responsible for notifying agencies of its final decision on how many additional access points the agency is to be allowed. As described earlier, several agencies indicated that they planned to request additional access points. However, even with this process in place, agencies may still be uncertain about the number of access points for which they have been approved if prior inconsistencies in communication from OMB resurface. For example, although one agency's request for additional access points was sent to OMB in April 2009, as of December 2009 agency officials indicated that they not been told whether the agency's request had been approved. Without consistent and timely communication of the results of agency requests for additional access points by OMB, agencies that requested additional access points will continue to face challenges with implementation of TIC.

---

<sup>27</sup>OMB, *Update on the Trusted Internet Connections Initiative*, M-09-32 (Washington, D.C.: Sept. 17, 2009).

---

In addition, DHS often did not promptly respond to agency questions about the technical aspects of securing TIC access points, further complicating agency implementation efforts. Although a few agencies that have asked DHS questions about the meaning of specific terms in the security capabilities or about guidance for implementation stated that DHS answered their questions effectively, four agencies stated that DHS has often been slow to respond to questions about the capabilities, or in some cases has not responded at all. Specifically, one agency noted that DHS took a year to produce answers to frequently asked questions that were generated in an inter-agency working group. Three other agencies told us that they still have not received answers to questions that they submitted to DHS on specific security capabilities such as data storage requirements, inspection of encrypted traffic, and participation in the Einstein program. DHS officials acknowledged that its communications with agencies had not been timely because it had limited staff at the beginning of the initiative.

Without consistent and timely communication from OMB and DHS, agencies may not be able to effectively execute plans for consolidating their external connections and securing their TIC access points.

**Ensuring that critical capabilities have been implemented.** DHS will be challenged to know whether access providers have adequately secured their access points because it does not directly test the capabilities in its compliance validation reviews. The National Institute of Standards and Technology states<sup>28</sup> that organizations should conduct assessments to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. During its reviews, DHS conducts document reviews, interviews, and observation of agency processes, but does not conduct direct testing of the capabilities to determine if they are effectively implemented, operating as intended, and achieving desired results. Even with this limited testing, five of the six reviews that DHS conducted showed that agencies had not fully implemented critical security capabilities that had previously been reported as implemented. However, without directly testing the

---

<sup>28</sup>National Institute of Standards and Technology: *Recommended Security Controls for Federal Information Systems*, Special Publication 800-53 Revision 3 (Gaithersburg, Md.: December 2007).



---

capabilities, DHS could be unaware of additional weaknesses that its more limited reviews may not have identified.

In addition, in at least three of the six reviews that it conducted at agencies, DHS did not evaluate all of the trusted connection locations. Specifically, in one agency's review, DHS evaluated only one of the agency's two security operations centers and one of its four TIC locations. According to DHS, the other center and three locations were not evaluated because the agency asserted that its other sites were identical to the ones evaluated. For another agency, DHS evaluated a security operations center and a telecommunications facility at the agency but did not examine controls at either of the agency's TIC access point locations. A third agency was only evaluated at one of its two TIC locations. DHS officials indicated that in designing the method for TIC compliance reviews, it was decided that the initial round of reviews would include only the most mature TIC locations and supporting network and operations centers. Without evaluating all agency locations in its compliance reviews, DHS cannot be assured that agencies have implemented critical capabilities at all locations.

Defining Requirements and Effective Communication Offer Lessons Learned for OMB and DHS as the Initiative Moves Forward

Agencies' experiences in implementing TIC offer valuable lessons learned for OMB and DHS.

**Defining requirements clearly and early prove useful for agency planning.** OMB and DHS did not always use sound program management principles when planning the TIC initiative. According to *The Standard for Program Management*, during the planning phase, program requirements should be developed before schedules are defined. However, OMB and DHS did not define certain fundamental requirements before establishing initial deadlines for the initiative. For example, DHS did not define the meaning of "external connection" until April 2009, 17 months after the initiative was announced and 10 months after the initial June 2008 deadline for reducing external connections to authorized levels. This resulted in DHS determining during a compliance validation review that one agency had not reported a number of external connections that needed to be consolidated. DHS officials acknowledged that this was due to confusion over the definition of what constituted an external connection. In addition, the technical security capabilities that would be required for access providers were still being defined when agencies developed their required initial implementation plans and were not finalized until April 2008, 5 months after the initiative was announced. As a result, several agencies stated that it was difficult for them to plan for TIC

---

implementation. In going forward, defining any key future requirements prior to establishing deadlines will be critical to the initiative's success.

**Collaborative meetings aided implementation.** DHS and OMB sponsored several collaborative meetings during the initiative that many agencies found beneficial for their implementation of TIC. Specifically, several agencies stated that the meetings of the inter-agency TIC technical working group were helpful. For example, one agency said that DHS provided updates about the initiative during the meetings. Another agency noted that the meetings provided additional specificity on aspects of the program. Several agencies also stated that the meetings provided a forum for agencies to discuss issues related to TIC with one another, allowing them to gain insight from other agencies. One of these agencies found the meetings to be helpful because it was able to provide feedback to DHS about the technical capabilities. Another agency noted that it had recently participated in conference calls with DHS that helped to address its technical questions related to implementing the critical capabilities. In the future, continuing such effective communication increases the chances of the initiative's success.

**Meeting business needs with a reduced number of connections is complex and time-consuming.** As indicated earlier, the 16 access provider agencies in our review are reporting that they are reducing and consolidating from 3,286 external connections. Reducing to the approved total of 32 TIC access points is a complex and time-consuming effort for most agencies. For example, one agency indicated that implementing the infrastructure required to support its mission would require 4 years to complete. Two other agencies noted that implementing the initiative required them to make significant changes to their existing network architecture. In addition, for several agencies, determining how to meet their business needs within the technical constraints of TIC has been a complex task. For example, three agencies stated that they needed more than two TIC access points to ensure that their networks would remain operational in the event of a disaster. One of these agencies explained that its high performance and capacity requirements would not be met with only two access points. The complex effort required for agencies to implement the initiative while still meeting their business needs has led to significant delays in agencies' plans for implementation. As indicated earlier, the access provider agencies have reported that they have consolidated fewer connections than they originally planned and have significantly revised their future plans for consolidation. Recognizing that agencies may desire more than two access points, as noted earlier, OMB

---

and DHS established a process for agencies to submit an evidence-based rationale for obtaining additional access points.

---

## DHS Has Deployed Einstein to Six Agencies, but Faces Challenges with Meeting Program Goals

Einstein is intended to provide DHS with an increased awareness of activity, including possible security incidents, on federal networks. As of September 2009, fewer than half of the 23 agencies had executed the required agreements with DHS, and Einstein 2 had been deployed to six agencies. Agencies that participated in Einstein 1 improved identification of incidents and mitigation of attacks, but DHS continues to face challenges with meeting the goals of the initiative.

---

## Einstein Is to Provide Increased Awareness of Activity on Agency Networks

The goal for Einstein is to provide US-CERT with a higher level of awareness of activity on federal networks. By implementing this initiative, DHS intended to achieve the following objectives:

- provide an automated process for collecting, correlating, and analyzing computer network traffic information from participating federal agencies;
- provide US-CERT with a means to observe potential malicious activity in computer network traffic entering and exiting participating agencies' computer networks;
- increase US-CERT's situational awareness of federal agency computer networks through correlation of activity across the entire federal enterprise; and
- incorporate intrusion detection technology (i.e., the Einstein sensors and signature-monitoring capabilities) capable of alerting US-CERT to the presence of malicious or potentially harmful computer network activity in federal agencies' network traffic.

---

DHS and Agencies Are Required to Take Various Actions before Einstein 2 Can Be Deployed

To accomplish these objectives, for Einstein 2, agencies are required to meet the following two requirements:<sup>29</sup>

- **Execute a memorandum of agreement with DHS.** This agreement establishes the responsibilities of deployment and operation of the sensor between the participating federal agency and DHS.
- **Execute a service level agreement with DHS.** This agreement defines the roles, responsibilities, and points of contact, as well as describes the services, hours of operation, and performance levels provided to the agency. It also requires agencies to update US-CERT regularly on the status of ongoing investigations related to alerts.

Agencies were required to report on the status of these agreements to DHS in September 2009.

In addition, the TIC access provider agencies are required to meet two additional requirements:

- **Execute an interconnection security agreement with DHS.** Describes the interconnection between the agency and DHS and the security controls required and implemented to protect the confidentiality, integrity, and availability of the systems and data. Agencies were required to report on their status in completing this agreement to DHS in September 2009.
- **Perform a site assessment.** Provides a technical description of the agency's network and how the network connects to the agency's Internet service providers.

Vendors that intend to provide TIC services to agencies under the Networx contract are also required to complete a memorandum of agreement, an interconnection security agreement, and a site assessment.

---

<sup>29</sup>For Einstein 1, DHS required participating agencies to complete a memorandum of agreement, interconnection security agreement, and a site assessment before receiving a sensor.

---

With the required agreements in place,<sup>30</sup> DHS is to deploy Einstein sensors to access provider agencies and Networx vendors. When deploying the sensors, DHS is to use a site deployment checklist to verify that the Einstein equipment is installed and configured appropriately. After the sensors are operational, US-CERT is to begin monitoring and analyzing results.

---

### Einstein 2 Has Been Deployed to Six Agencies, but DHS and Agencies Did Not Always Complete Required Activities

As of September 2009, DHS had deployed Einstein 2 at six access provider agencies included in our review and at three Networx vendors. According to DHS, the sensors at five of the six agencies were operational as of September 2009; it had not activated the sensors at one agency because it was waiting for the agency to complete required agreements.

Agencies that had operational sensors had completed certain required agreements, but not all agencies had executed all required agreements. All five agencies with operational sensors had executed memorandums of agreement and interconnection security agreements with DHS as required. However, three of the five agencies had not executed service level agreements. According to DHS officials, these agencies were still in the process of negotiating the agreements. However, the agreements define key requirements for the initiative, including how US-CERT is to notify agencies of potential incidents and how agencies are to respond to these notifications, including what information must be provided to US-CERT in support of investigations related to Einstein alerts. Without these agreements in place between agencies and DHS, agencies may not receive the information needed to address security incidents detected by Einstein, and DHS may not obtain the information it needs from agencies in order to fully meet the objective of improving situational awareness.

DHS and the agencies also did not always complete deployment checklists. Although all five of the agencies had performed required site assessments, the site deployment checklists for two agencies had not been signed by officials from the agency or from DHS verifying that the sensors had been installed and configured appropriately. As a result, DHS and agency management cannot be assured that the Einstein equipment has been installed and configured appropriately.

---

<sup>30</sup> Although agencies are required to complete a service level agreement, DHS officials stated that it is not necessary for it to be completed before the Einstein sensors are deployed.

---

Because these sensors had only recently been deployed, we did not evaluate the extent to which US-CERT was collecting and analyzing data and reporting alerts to agencies for Einstein 2.

Not all of the remaining 17 agencies reported their status toward submitting required agreements to DHS in September 2009. Only a few have reported completing required agreements with DHS, while several have not yet reported their plans for submitting agreements.<sup>31</sup> Specifically:

- Four agencies reported that they had completed and submitted their memorandums of agreement to DHS, and 4 reported that they expected to submit them within a year; however, nine did not project a date by which they expected to submit them.
- One agency reported that it had submitted its service level agreement to DHS, and 4 reported that they expected to submit them between December 2009 and September 2010; however, 12 did not project a date by which they expected to submit the agreement.
- Two of the 10 remaining agencies required to execute interconnection security agreements<sup>32</sup> reported that they had submitted them to DHS, and 1 reported that it expected to submit the agreement within the next year; however, 7 did not project a date by which they expected to submit the agreements.

Although DHS required agencies to report their status toward executing required agreements in September 2009, it did not establish milestones for agencies to submit the agreements. According to *The Standard for Program Management*, the actual completion of program activities and milestones should be tracked against a planned timeline in order to ensure that the program produces its required deliverables on time. However, DHS had not established any milestones for agencies to submit these agreements. As indicated earlier, these agreements establish key responsibilities and controls that are necessary for successful operation of the sensors. Without establishing milestones for these agreements, DHS could face delays in deploying and activating Einstein sensors.

---

<sup>31</sup>One access provider agency did not submit its updated plan to DHS in September 2009.

<sup>32</sup>The seven agencies seeking service from other access providers are not required to execute interconnection security agreements.

---

## Einstein Has Proven Beneficial to Providing Security, but DHS Faces Ongoing Challenges with Meeting Program Goals

Agencies have benefited from Einstein alerts, and their experiences have provided DHS with valuable lessons; however, DHS may be challenged in meeting program goals as the system is deployed at more agencies.

### Einstein Provided Security Benefits for Agencies

Although Einstein 2 has only been deployed at 6 agencies, the 12 agencies that participated in Einstein 1 realized benefits in the following areas:

**Identifying incidents.** US-CERT provided alerts to agencies from its analysis of the data from the Einstein 1 sensors, which contained information about potential cyber attacks or incidents against the agency's networks. Several agencies observed that the alerts from US-CERT were helpful or contained useful information about potential incidents, including information that could be used to trace potential incidents to specific locations on the network. For some agencies, Einstein identified incidents that agencies' intrusion detection systems had not found, increasing their ability to mitigate potential attacks.

**Providing cross-agency view.** For Einstein 1, US-CERT provided reports based on a correlation of sensor data from all of the participating agencies. Several agencies said US-CERT's ability to aggregate Einstein data from multiple agencies was beneficial for identifying potential attacks against government networks.

**Using sensor data.** In addition to receiving alerts generated by US-CERT's analysis, agencies had the ability to access the sensor data directly via a Web portal. Several agencies indicated that they used this data to look for potential incidents on their own.

### DHS Faces Challenges with Meeting Einstein Goals and Providing Adequate Analysis

As DHS deploys Einstein across the government, it faces the following challenges:

**Understanding whether alerts are valid.** Although one of the objectives of Einstein is to improve situational awareness of activity across the federal government, DHS will be challenged in understanding the extent to which this objective is being met because it lacks performance measures for Einstein 2 that address whether or not agencies report that the alerts represent actual incidents. For Einstein 1, agencies did not always inform US-CERT of how they responded to the alerts. As a result, US-CERT did not know whether these alerts represented false

---

positives or actual incidents. We have previously reported that performance measures are most meaningful when they are linked with organizational goals.<sup>33</sup> DHS's performance measures for Einstein 2 indicate the time required for the system to detect known cyber events and to generate automated notifications once the events are detected, but they do not indicate agencies' responses to alerts. Establishing such measures would help DHS better understand whether the alerts are valid, helping it to better determine the extent to which the initiative is meeting its objective of improving situational awareness.

**Having staff with required skills to monitor and analyze data.** DHS will be challenged to have staff with the appropriate skills to fulfill its analysis and incident response mission as Einstein 2 is deployed across the government. As more agencies receive sensors, the amount of data that US-CERT will be responsible for analyzing will drastically increase. DHS recognizes that staff with appropriate analytical skills will be required in order to handle the increased workload, but it has not developed a staffing plan to address its need to acquire and retain qualified analysts at US-CERT. Although the department announced in October 2009 that it plans to hire up to 1,000 new cybersecurity professionals over the next 3 years, we previously reported in July 2008 that obtaining and retaining adequately trained cyber analysts is an ongoing challenge to US-CERT that hinders its ability to respond to increasingly fast, nimble, and sophisticated cyber attacks. At that time, we recommended that the department address the challenges that have impeded it from expeditiously hiring sufficiently trained cyber analysts and developing strategies for hiring and retaining highly qualified cyber analysts.<sup>34</sup> Although DHS indicated that it plans to expedite the hiring and onboarding process for new analysts and to offer appropriate training opportunities for its analysts, it has not yet provided evidence that it has taken these actions. Until DHS addresses our prior recommendation by developing strategies for hiring and retaining cyber analysts, US-CERT may lack staff with appropriate skills to analyze the Einstein data, increasing the risk that attacks against federal networks could go undetected.

---

<sup>33</sup>GAO, *Information Security: Concerted Effort Needed to Improve Federal Performance Measures*, [GAO-09-617](#) (Washington, D.C.: Sept. 14, 2009).

<sup>34</sup>GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, [GAO-08-588](#) (Washington, D.C.: July 31, 2008).



---

Additional Information from  
US-CERT Helped Agencies,  
Providing Valuable Lessons  
Learned

Agencies' experiences with the initial version of Einstein provided DHS with lessons learned for future versions of the initiative.

**Detailed and timely information from alerts proved useful.** Several agencies' experiences with Einstein 1 improved over time because information provided by US-CERT increased in its timeliness and detail. Although some agencies said that the alerts and reports that US-CERT provided were not always timely and useful, a few agencies observed that the information had improved over time. For example, one agency stated that the alerts lacked sufficient contextual information, making it difficult to determine whether the alerts were identifying false positives or actual incidents; however, several agencies indicated that the alerts had since improved in their usefulness. In addition, although several agencies noted that the alerts were not very timely when the sensors were first installed, a few indicated that the timeliness had improved for more recent alerts. Going forward, continuing to provide appropriate and timely information from the alerts will prove useful for agencies.

**Access to sensor data proved useful for agencies.** Further, several agencies that had direct access to the flow records from the Einstein sensor found that it was helpful in detecting potential incidents. DHS stated that all agencies participating in Einstein 2 will also have access to the flow data, which could provide similar benefits. However, not all agencies were aware that they would have access to this data. Making them aware of this and of the data's possible benefits could aid agencies in improving their monitoring of potential incidents.

---

## Conclusions

TIC and Einstein are ambitious efforts that can help improve security and situational awareness across the federal government. However, in implementing the initiatives, federal agencies have faced challenges. For TIC, OMB did not consistently communicate the number of access points for which agencies had been approved, and DHS did not always provide timely answers to agency questions about technical capabilities. In addition, because DHS does not conduct direct testing of the capabilities or evaluate all possible locations in its validation reviews, it cannot be assured that all critical capabilities have been implemented. For Einstein, the initiative could fail to fully meet the objective of increasing US-CERT's situational awareness because DHS did not always ensure that key agreements were executed with agencies. DHS could also be challenged in determining whether the initiative is meeting this objective without performance measures that indicate whether the alerts provided to agencies represent actual incidents. Without improvements in program

---

management and communication from OMB and DHS, federal agencies will continue to be faced with challenges in implementing these initiatives that could ultimately jeopardize their ability to reduce and secure Internet connections.

With agencies still in the process of implementing TIC and DHS in the early stages of deploying Einstein 2, the success of such large-scale initiatives will be in large part determined by the extent to which DHS, OMB, and other federal agencies work together to address the challenges of these efforts and to apply lessons learned during the initial stages of implementation. Although this will not guarantee the success of TIC and Einstein, doing so will enhance the chances that the initiatives will meet their goals of reducing, consolidating, and securing federal Internet connections.

---

## Recommendations for Executive Action

In order to ensure that federal agencies continue to have adequate information about the number of connections for which they have been approved, we recommend that the Director of OMB take the following two actions:

- Communicate its final decisions on agency requests for additional TIC access points in a consistent and timely manner.
- Assess the efficacy of, and take steps to apply as appropriate, the lesson learned during the initial implementation of TIC regarding the need to define future requirements before establishing deadlines.

In addition, in order to further ensure that federal agencies have adequate, sufficient, and timely information to successfully meet the goals and objectives of the TIC and Einstein programs, we recommend that the Secretary of Homeland Security take the following six actions:

- Provide agencies with timely responses to their questions seeking clarification on TIC security capabilities.
- Enhance TIC compliance validations by including (1) direct testing and evaluation of the critical capabilities and (2) evaluation of the capabilities at all agency TIC locations.
- Before activating Einstein sensors, ensure that both DHS and participating agencies (1) execute required service level agreements and (2) sign site deployment checklists.

- 
- Establish milestones for agencies to submit required Einstein agreements.
  - To better understand whether Einstein alerts are valid, develop additional performance measures that indicate how agencies respond to alerts.
  - Assess the efficacy of, and take steps to apply as appropriate, lessons learned during the initial implementation of these initiatives such as the need to (1) define future requirements for TIC before establishing deadlines and (2) make agencies aware of their ability to access Einstein flow data.

---

## Agency Comments and Our Evaluation

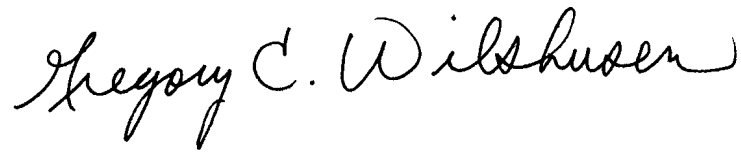
We provided a draft of this report to OMB and DHS for their review and comment. In providing e-mail comments on a draft of this report, the lead information technology policy analyst from OMB's Office of E-Government and Information Technology stated that OMB concurred with the report's findings, conclusions, and two recommendations addressed to OMB. In e-mail comments provided by an audit liaison from DHS's Office of Cybersecurity and Communications, DHS concurred with the six recommendations addressed to DHS. DHS also provided technical comments, which we have incorporated into this report as appropriate. We also provided a draft of this report to the 22 other agencies included in our review. Of the 22, 15 responded that they did not have any comments; 1 provided technical comments, which we addressed as appropriate; and 6 did not respond.

---

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its date. At that time, we will send copies to interested congressional committees, secretaries of the Departments of Agriculture, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Attorney General; the administrators of the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, Small Business Administration, and the U.S. Agency for International Development; the Chairman of the Nuclear Regulatory Commission; the Commissioner of the Social Security Administration; and the directors of the National Science Foundation, Office of Management and Budget, and Office of Personnel Management. The report also is available at no charge on the GAO Web site at <http://www.gao.gov>.

---

If you or your staff have any questions regarding this report, please contact me at (202) 512-6244 or at [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, prominent 'G' and 'W'.

Gregory C. Wilshusen  
Director, Information Security Issues

---

# Appendix I: Objectives, Scope, and Methodology

---

The scope of our review covered two initiatives: Trusted Internet Connections (TIC) and the National Cybersecurity Protection System (NCPS) program, operationally known as Einstein. For each initiative, our objectives were to (1) identify their goals, objectives, and requirements; (2) determine the status of the actions federal agencies have taken, or plan to take, to implement them; and (3) identify the benefits, challenges, and lessons learned in implementing each initiative.

For TIC, to address the first objective, we obtained and reviewed applicable policies and memorandums issued by the Office of Management and Budget (OMB) and guidance, reports, and other documentation provided by the Department of Homeland Security (DHS). We also held discussions with OMB and DHS representatives concerning the goals, objectives, and requirements of the initiative. To understand the options for agencies seeking to acquire TIC services through the Networkx contract, we obtained and reviewed relevant documents regarding Networkx and interviewed officials from the General Services Administration.

To address the second objective for TIC, we reviewed statements of capability, plans of action and milestones, and other relevant documents for 23 of the 24 agencies<sup>1</sup> listed in the Chief Financial Officers Act of 1990<sup>2</sup> to determine if reporting requirements were met. We also reviewed these documents to determine reported progress toward the reduction and consolidation of external connections and implementation of critical capabilities and analyzed them to estimate the overall progress reported by agencies. We also reviewed documentation from DHS to determine whether agencies submitted the required documents. In addition, we reviewed the results of six TIC Compliance Validation reviews and interviewed officials from DHS to understand how the department assesses agencies' degree of compliance with TIC and to determine the extent to which the information reported in agency plans of action and milestones was accurate.

To address the third objective for TIC, we interviewed officials from each agency, DHS, and OMB. In addition, we obtained written responses to follow-up questions from each agency. We also examined plans of action

---

<sup>1</sup>The Department of Defense was not included in our review because it was not required to implement TIC or Einstein.

<sup>2</sup>31 U.S.C. §901(b).

and milestones and other relevant documents from each agency and reviewed policies and guidance from OMB and DHS to identify any additional benefits, challenges, or lessons learned. Further, we interviewed officials from agency inspectors general to obtain information on any benefits, challenges, or lessons learned that they had identified related to the initiative.

For Einstein, to address the first objective, we obtained and reviewed applicable policies, guidance, and other documentation provided by DHS. We also held discussions with DHS officials concerning the goals, objectives, and requirements of the initiative.

To address the second objective for Einstein, we reviewed plans of action and milestones for each agency to determine whether reporting requirements were met. In addition, we examined required agreements and site assessments for the six agencies where Einstein 2 was deployed to verify their completion. We also interviewed officials and obtained written information from DHS and from each agency to obtain additional information on the status of implementation.

To address the third objective for Einstein, we interviewed officials from DHS and from each agency. In addition, we obtained and reviewed written responses to follow-up questions from each agency. We also examined policies, guidance, and other documentation from DHS to identify any additional benefits, challenges, or lessons learned. Further, we interviewed officials from agency inspectors general to obtain information on any benefits, challenges, or lessons learned that they had identified related to the initiative.

We conducted this performance audit from December 2008 to March 2010 in Washington, D.C., in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

# Appendix II: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov

---

## Staff Acknowledgments

In addition to the individual named above, Jeffrey Knott (Assistant Director); John Bainbridge; William Cook; Kami Corbett; Neil Doherty; Rebecca Eyler; Nancy Glover; Valerie Hopkins; Lee McCracken; Zsarog Powe; and Shawn Ward made key contributions to this report.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

