United States Government Accountability Office

GAO

Report to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

July 2008

CYBER ANALYSIS AND WARNING

DHS Faces Challenges in Establishing a Comprehensive National Capability

This Report Is Temporarily Restricted Pending Official Public Release.

GAO-08-588

July 31, 2008

CYBER ANALYSIS AND WARNING

DHS Faces Challenges in Establishing a Comprehensive National Capability

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-588, a report to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Cyber analysis and warning capabilities are critical to thwarting computer-based (cyber) threats and attacks. The Department of Homeland Security (DHS) established the United States Computer Emergency Readiness Team (US-CERT) to, among other things, coordinate the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. GAO's objectives were to (1) identify key attributes of cyber analysis and warning capabilities, (2) compare these attributes with US-CERT's current capabilities to identify whether there are gaps, and (3) identify US-CERT's challenges to developing and implementing key attributes and a successful national cyber analysis and warning capability. To address these objectives, GAO identified and analyzed related documents, observed operations at numerous entities, and interviewed responsible officials and experts.

What GAO Recommends

GAO is making 10 recommendations to the Secretary of Homeland Security to implement key attributes and address challenges. DHS concurred with 9 recommendations. It took exception to GAO's recommendation to ensure distinct and transparent lines of authority and responsibilities between its organizations, stating it had done this in a concept-of-operations document. However, this document is still in draft, and DHS has not established a date for it to be finalized and implemented.

To view the full product, including the scope and methodology, click on GAO-08-588. For more information, contact Dave Powner at 202-512-9286 or pownerd@gao.gov.

What GAO Found

Cyber analysis and warning capabilities include (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. GAO identified 15 key attributes associated with these capabilities, as shown in the following table:

Key Attributes of Cyber Analysis and Warning

Capability	Attribute
Monitoring	• Establish a baseline understanding of network assets and normal network traffic volume and flow • Assess risks to network assets • Obtain internal information on network operations via technical tools and user reports • Obtain external information on threats, vulnerabilities, and incidents • Detect anomalous activities
Analysis	• Verify that an anomaly is an incident (threat of attack or actual attack) • Investigate the incident to identify the type of cyber attack, estimate impact, and collect evidence • Identify possible actions to mitigate the impact of the incident • Integrate results into predictive analysis of broader implications or potential future attack
Warning	• Develop attack and other notifications that are targeted and actionable • Provide notifications in a timely manner • Distribute notifications using appropriate communications methods
Response	• Contain and mitigate the incident • Recover from damages and remediate vulnerabilities • Evaluate actions and incorporate lessons learned

Source: GAO analysis.

While US-CERT's cyber analysis and warning capabilities include aspects of each of the key attributes, they do not fully incorporate all of them. For example, as part of its monitoring, US-CERT obtains information from numerous external information sources; however, it has not established a baseline of our nation's critical network assets and operations. In addition, while it investigates if identified anomalies constitute actual cyber threats or attacks as part of its analysis, it does not integrate its work into predictive analyses. Further, it provides warnings by developing and distributing a wide array of notifications; however, these notifications are not consistently actionable or timely.

US-CERT faces a number of newly identified and ongoing challenges that impede it from fully incorporating the key attributes and thus being able to coordinate the national efforts to prepare for, prevent, and respond to cyber threats. The newly identified challenge is creating warnings that are consistently actionable and timely. Ongoing challenges that GAO previously identified, and made recommendations to address, include employing predictive analysis and operating without organizational stability and leadership within DHS, including possible overlapping roles and responsibilities. Until US-CERT addresses these challenges and fully incorporates all key attributes, it will not have the full complement of cyber analysis and warning capabilities essential to effectively performing its national mission.

Contents

Figures

Abbreviations

CERT/CC	CERT Coordination Center
DHS	Department of Homeland Security
DOD	Department of Defense
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSPD	Homeland Security Presidential Directive
ISAC	information sharing and analysis center
NCRCG	National Cyber Response Coordination Group
NCSD	National Cyber Security Division
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
US-CERT	United States Computer Emergency Readiness Team

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 31, 2008

The Honorable James R. Langevin
Chairman
The Honorable Michael T. McCaul
Ranking Member
Subcommittee on Emerging Threats, Cybersecurity, and
Science and Technology
Committee on Homeland Security
House of Representatives

The rapid increase in computer connectivity has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to our nation's computer-reliant critical operations. Establishing analytical and warning capabilities is essential to thwarting computer-based, or cyber, threats and attacks. Cyber analysis and warning capabilities include (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat.

Federal law and policy direct the Department of Homeland Security (DHS) to establish such capabilities for our nation. To fulfill this requirement, the department established the United States Computer Emergency Readiness Team (US-CERT) to develop and implement these capabilities and, in doing so, coordinate the nation's efforts to prepare for, prevent, and respond to cyber threats and attacks.

Our objectives were to (1) identify key attributes of cyber analysis and warning capabilities, (2) compare these attributes with US-CERT's current analysis and warning capabilities to identify whether there are gaps, and (3) identify US-CERT's challenges to developing and implementing key attributes and a successful national cyber analysis and warning capability. To identify key attributes, we identified and analyzed relevant laws, strategies, policies, reports, and studies; observed cyber analysis and warning operations at numerous entities; and interviewed responsible

officials and experts from federal and nonfederal entities.[1] To determine US-CERT's current capabilities and related challenges, we analyzed DHS's policies, procedures, and program plans and interviewed relevant officials. Appendix I provides further details on our objectives, scope, and methodology.

We conducted this performance audit from June 2007 to July 2008 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.

Results in Brief

Cyber analysis and warning typically encompasses four key capabilities: monitoring, analysis, warning, and response. Monitoring system and communication networks includes activities to detect cyber threats, attacks, and vulnerabilities. Analysis involves taking the information gathered from monitoring and hypothesizing about what the threat or attack might be, investigating it, and identifying any impact and, if necessary, mitigation steps. Warning includes alerting recipients about potential or imminent, as well as ongoing, cyber threats or attacks. Response includes containing and recovering from cyber incidents that occur. Our research and past experience identified 15 key attributes associated with these cyber analysis and warning capabilities, as shown in the following table:

[1]Nonfederal entities include state and local governments, private sector entities, and academic institutions.

Table 1: Attributes of Cyber Analysis and Warning

Capability	Attribute
Monitoring	Establish a baseline understanding of network assets and normal network traffic volume and flow
	Assess risks to network assets
	Obtain internal information on network operations via technical tools and user reports
	Obtain external information on threats, vulnerabilities, and incidents
	Detect anomalous activities
Analysis	Verify that an anomaly is an incident (threat of attack or actual attack)
	Investigate the incident to identify the type of cyber attack, estimate impact, and collect evidence
	Identify possible actions to mitigate the impact of the incident
	Integrate results into predictive analysis of broader implications or potential future attack
Warning	Develop attack and other notifications that are targeted and actionable
	Provide notifications in a timely manner
	Distribute notifications using appropriate communications methods
Response	Contain and mitigate the incident
	Recover from damages and remediate vulnerabilities
	Evaluate actions and incorporate lessons learned

Source: GAO analysis.

While US-CERT's cyber analysis and warning capabilities include aspects of each of the key attributes, they do not fully incorporate all of them. For example, as part of its monitoring, US-CERT obtains information from numerous external information sources; however, it has not established a comprehensive baseline of our nation's critical computer-reliant critical assets and network operations. In addition, while it investigates if identified anomalies constitute actual cyber threats or attacks as part of its analysis, the organization does not integrate its work into predictive analyses, nor does it have the analytical or technical resources to analyze multiple, simultaneous cyber incidents. The organization also provides warnings by developing and distributing a wide array of attack and other notifications; however, these notifications are not consistently actionable or timely—providing the right information to the right persons or groups as early as possible to give them time to take appropriate action. Further, while it responds to a limited number of affected entities in their efforts to contain and mitigate an attack, recover from damages, and remediate vulnerabilities, the organization does not possess the resources to handle multiple events across the nation.

US-CERT faces a number of newly identified and ongoing challenges that impede it from fully implementing the key attributes and in turn establishing cyber analysis and warning capabilities essential to

coordinating the national effort to prepare for, prevent, and respond to cyber threats. The newly identified challenge is creating warnings that are actionable and timely—US-CERT does not consistently issue warning and other notifications that its customers find useful. Ongoing challenges that we previously identified and made recommendations to address are

- employing predictive cyber analysis—the organization has not established the ability to determine broader implications from ongoing network activity, predict or protect against future threats, or identify emerging attack methods;

- developing more trusted relationships to encourage information sharing—federal and nonfederal entities are reluctant to share information because US-CERT and these parties have yet to develop close working and trusted relationships that would allow the free flow of information;

- having sufficient analytical and technical capabilities—the organization has difficulty hiring and retaining adequately trained staff and acquiring supporting technology tools to handle a steadily increasing workload; and

- operating without organizational stability and leadership within DHS—the department has not provided the sustained leadership to make cyber analysis and warning a priority. This is due in part to frequent turnover in key management positions that currently also remain vacant. In addition, US-CERT's role as the central provider of cyber analysis and warning may be diminished by the creation of a new DHS center at a higher organizational level.

Until DHS addresses these challenges and fully incorporates all key attributes into its capabilities, it will not have the full complement of cyber analysis and warning capabilities essential to effectively performing its national mission.

Accordingly, we are making 10 recommendations to the Secretary of Homeland Security to improve DHS's cyber analysis and warning capabilities by implementing key cyber analysis and warning attributes and addressing the challenges, including

- developing close working and more trusted relationships with federal and nonfederal entities that would allow the free flow of information,

- expeditiously hiring sufficiently trained staff and acquiring supporting technology tools to handle the steadily increasing workload,

- ensuring consistent notifications that are actionable and timely,
- filling key management positions to provide organizational stability and leadership, and
- ensuring that there are distinct and transparent lines of authority and responsibility assigned to DHS organizations with cybersecurity roles and responsibilities.

In written comments on a draft of this report (see app. II), the department concurred with 9 of our 10 recommendations. It also described actions planned and under way to implement these recommendations. DHS took exception to 1 recommendation, stating that it had developed a concept-of-operations document that clearly defined roles and responsibilities for key DHS organizations. However, this document is still in draft, and the department has yet to establish a date for it to be finalized and implemented.

Background

Increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, they are accompanied by significant risks to the nation's computer systems and to the critical operations and infrastructures that those systems support.[2]

Cyber Threats and Incidents Adversely Affect the Nation's Critical Infrastructure

Different types of cyber threats from numerous sources may adversely affect computers, software, a network, an agency's operations, an industry, or the Internet itself. Cyber threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks. A targeted attack

[2]Critical infrastructure is systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. There are 18 critical infrastructure sectors: agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, information technology, national monuments and icons, nuclear reactors, materials and waste, postal and shipping, public health and health care, transportation systems, and water.

occurs when a group or individual specifically attacks a cyber asset. An untargeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or malware is released on the Internet with no specific target.

Threats to the Nation's Critical Infrastructure Are Proliferating

There is increasing concern among both government officials and industry experts regarding the potential for a cyber attack on the national critical infrastructure, including the infrastructure's control systems. The Department of Defense (DOD) and the Federal Bureau of Investigation, among others, have identified multiple sources of threats to our nation's critical infrastructure, including foreign nation states engaged in information warfare, domestic criminals, hackers, virus writers, and disgruntled employees working within an organization. In addition, there is concern about the growing vulnerabilities to our nation as the design, manufacture, and service of information technology have moved overseas.[3] For example, according to media reports, technology has been shipped to the United States from foreign countries with viruses on the storage devices.[4] Further, U.S. authorities are concerned about the prospect of combined physical and cyber attacks, which could have devastating consequences. For example, a cyber attack could disable a security system in order to facilitate a physical attack. Table 2 lists sources of threats that have been identified by the U.S. intelligence community and others.

[3]Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence* (Feb. 5, 2008).

[4]Robert McMillan, "Seagate Ships Virus-Laden Hard Drives," InfoWorld (San Francisco, California: InfoWorld Media Group, Nov. 12, 2007), http://www.infoworld.com/article/07/11/12/Seagate-ships-virus-laden-hard-drives_1.html (accessed Apr. 9, 2008).

Table 2: Sources of Emerging Cybersecurity Threats

Threat	Description
Bot-network operators	Bot-network operators take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks (See Table 3 for definitions). The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or servers to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Federal Bureau of Investigation, the Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center.

The nation's critical infrastructure operates in an environment of increasing and dynamic threats, and adversaries are becoming more agile and sophisticated. Terrorists, transnational criminals, and intelligence services use various cyber tools that can deny access, degrade the integrity

of, intercept, or destroy data and jeopardize the security of the nation's critical infrastructure (see table 3).

Table 3: Types of Cyber Attacks

Type of attack	Description
Denial of service	A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.
Distributed denial of service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Phishing	The creation and use of e-mails and Web sites—designed to look like those of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then use that information for criminal purposes, such as identity theft and fraud.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
Vishing	A method of phishing based on voice-over-Internet Protocol technology and open-source call center software that have made it inexpensive for scammers to set up phony call centers and criminals to send e-mail or text messages to potential victims, saying there has been a security problem and they need to call their bank to reactivate a credit or debit card, or send text messages to cell phones, instructing potential victims to contact fake online banks to renew their accounts.
War driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no available fixes.

Source: GAO analysis of data from GAO and industry reports.

Cyber Incidents Have Caused Serious Damage

The growing number of known vulnerabilities increases the potential number of attacks. By exploiting software vulnerabilities, hackers and others who spread malicious code can cause significant damage, ranging

from defacing Web sites to taking control of entire systems and thereby being able to read, modify, or delete sensitive information; disrupt operations; launch attacks against other organizations' systems; or destroy systems. Reports of attacks involving critical infrastructure demonstrate that a serious attack could be devastating, as the following examples illustrate.

- In June 2003, the U.S. government issued a warning concerning a virus that specifically targeted financial institutions. Experts said the BugBear.b virus was programmed to determine whether a victim had used an e-mail address for any of the roughly 1,300 financial institutions listed in the virus's code. If a match was found, the software attempted to collect and document user input by logging keystrokes and then provide this information to a hacker, who could use it in attempts to break into the banks' networks.[5]

- In August 2006, two Los Angeles city employees hacked into computers controlling the city's traffic lights and disrupted signal lights at four intersections, causing substantial backups and delays. The attacks were launched prior to an anticipated labor protest by the employees.[6]

- In October 2006, a foreign hacker penetrated security at a water filtering plant in Harrisburg, Pennsylvania. The intruder planted malicious software that was capable of affecting the plant's water treatment operations.[7]

- In May 2007, Estonia was the reported target of a denial-of-service cyber attack with national consequences. The coordinated attack created mass outages of its government and commercial Web sites.[8]

- In March 2008, the Department of Defense reported that in 2007 computer networks operated by Defense, other federal agencies, and defense-related

[5]GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

[6]GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-08-119T (Washington, D.C.: Oct. 17, 2007).

[7]GAO-08-119T.

[8]Computer Emergency Response Team of Estonia, "Malicious Cyber Attacks Against Estonia Come from Abroad," April 29, 2007, and Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference, April 8, 2008.

think tanks and contractors were targets of cyber warfare intrusion techniques. Although those responsible were not definitively substantiated, the attacks appeared to have originated in China.[9]

As these examples illustrate, attacks resulting in the incapacitation or destruction of the nation's critical infrastructures could have a debilitating impact on national and economic security and on public health and safety.

Federal Law and Policy Establish the Need for National Cyber Analysis and Warning

To protect the nation's critical computer-dependent infrastructures against cyber threats and attacks, federal law and policy have identified the need to enhance cybersecurity and establish cyber analytical and warning capabilities, which are sometimes referred to as "indications and warnings." The laws and policies include (1) the Homeland Security Act of 2002, (2) the National Strategy to Secure Cyberspace, (3) Homeland Security Presidential Directive 7, and (4) the National Response Framework. In addition, the President issued in January 2008 Homeland Security Presidential Directive 23, which, according to US-CERT officials, has provisions that affect cyber analysis and warning efforts of the federal government.

Homeland Security Act of 2002

The Homeland Security Act of 2002 established the Department of Homeland Security and gave it lead responsibility for preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing the damage and assisting in recovery from attacks that do occur.[10] The act assigned the department, among other things, a number of critical infrastructure protection responsibilities, including gathering of threat information, including cyber-related, from law enforcement, intelligence sources, and other agencies of the federal, state, and local governments and private sector entities to identify, assess, and understand threats; carrying out assessments of the vulnerabilities of key resources to determine the risks posed by attacks; and integrating information, analyses, and vulnerability assessments in order to identify priorities for protection. In addition, the department is responsible for disseminating, as appropriate, information that it analyzes—both within the department and to other federal, state, and local government agencies

[9]Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2008.*

[10]Homeland Security Act of 2002, Pub. L. 107-296 (Nov. 25, 2002).

and private sector entities—to assist in the deterrence, prevention, preemption of, or response to terrorist acts.

National Strategy to Secure Cyberspace

The National Strategy to Secure Cyberspace proposes that a public/private architecture be provided for analyzing, warning, and managing incidents of national significance.[11] The strategy states that cyber analysis includes both (1) tactical analytical support during a cyber incident and (2) strategic analyses of threats. Tactical support involves providing current information on specific factors associated with incidents under investigation or specific identified vulnerabilities. Examples of tactical support include analysis of (1) a computer virus delivery mechanism to issue immediate guidance on ways to prevent or mitigate damage related to an imminent threat or (2) a specific computer intrusion or set of intrusions to determine the perpetrator, motive, and method of attack. Strategic analysis is predictive in that it looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential future threat of national importance. For example, strategic analyses may identify long-term vulnerability and threat trends that provide advance warnings of increased risk, such as emerging attack methods. Strategic analyses are intended to provide policymakers with information that they can use to anticipate and prepare for attacks, thereby diminishing the damage from such attacks.

Homeland Security Presidential Directive 7

Homeland Security Presidential Directive 7 (HSPD 7) directs DHS to, among other things, serve as the focal point for securing cyberspace. This includes analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for critical infrastructure information systems.[12] It also directs DHS to develop a national indications and warnings architecture for infrastructure protection and capabilities, including cyber, that will facilitate an understanding of baseline infrastructure operations, the identification of indicators and precursors to an attack, and create a surge capacity for detecting and analyzing patterns of potential attacks.

[11]The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

[12]The White House, *Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection* (Washington, D.C.: Dec. 17, 2003).

In May 2005, we reported that DHS has many cybersecurity-related roles and responsibilities, including developing and enhancing national cyber analysis and warning capabilities.[13] However, we found that DHS had not fully addressed all its cybersecurity-related responsibilities and that it faced challenges that impeded its ability to fulfill its responsibilities. These challenges included having organizational stability and authority, hiring employees, establishing information sharing and effective partnerships, and developing strategic analysis and warning. We made recommendations to the Secretary of Homeland Security to engage appropriate stakeholders to prioritize key cybersecurity responsibilities, develop a prioritized list of key activities to addressing underlying challenges, and identify performance measures and milestones for fulfilling its responsibilities and for addressing its challenges. We did not make new recommendations regarding cyber-related analysis and warning because our previous recommendations had not been fully implemented. Specifically, in 2001, we recommended that responsible executive branch officials and agencies establish a capability for strategic analysis of computer-based threats, including developing a methodology, acquiring expertise, and obtaining infrastructure data.[14]

National Response Framework

The National Response Framework, issued by DHS in January 2008, provides guidance to coordinate cyber incident response among federal entities and, upon request, state and local governments and private sector entities.[15] Specifically, the Cyber Incident Annex describes the framework for federal cyber incident response in the event of a cyber-related incident of national significance affecting the critical national processes. Further, the annex formalizes the National Cyber Response Coordination Group (NCRCG). As established under the preceding National Response Plan, the NCRCG continues to be cochaired by DHS's National Cyber Security Division (NCSD), the Department of Justice's Computer Crime and Intellectual Property Section, and the DOD. It is to bring together officials from all agencies that have responsibility for cybersecurity and the sector-specific agencies identified in HSPD 7. The group coordinates intergovernmental and public/private preparedness and response to and recovery from national-level cyber incidents and physical attacks that have

[13]GAO-05-434.

[14]GAO, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: Apr. 25, 2001).

[15]Department of Homeland Security, *National Response Framework* (Washington, D.C.: January 2008).

significant cyber-related consequences. During and in anticipation of such an incident, the NCRCG's senior-level membership is responsible for providing subject matter expertise, recommendations, and strategic policy support and ensuring that the full range of federal capabilities is deployed in a coordinated and effective fashion.

Homeland Security Presidential Directive 23

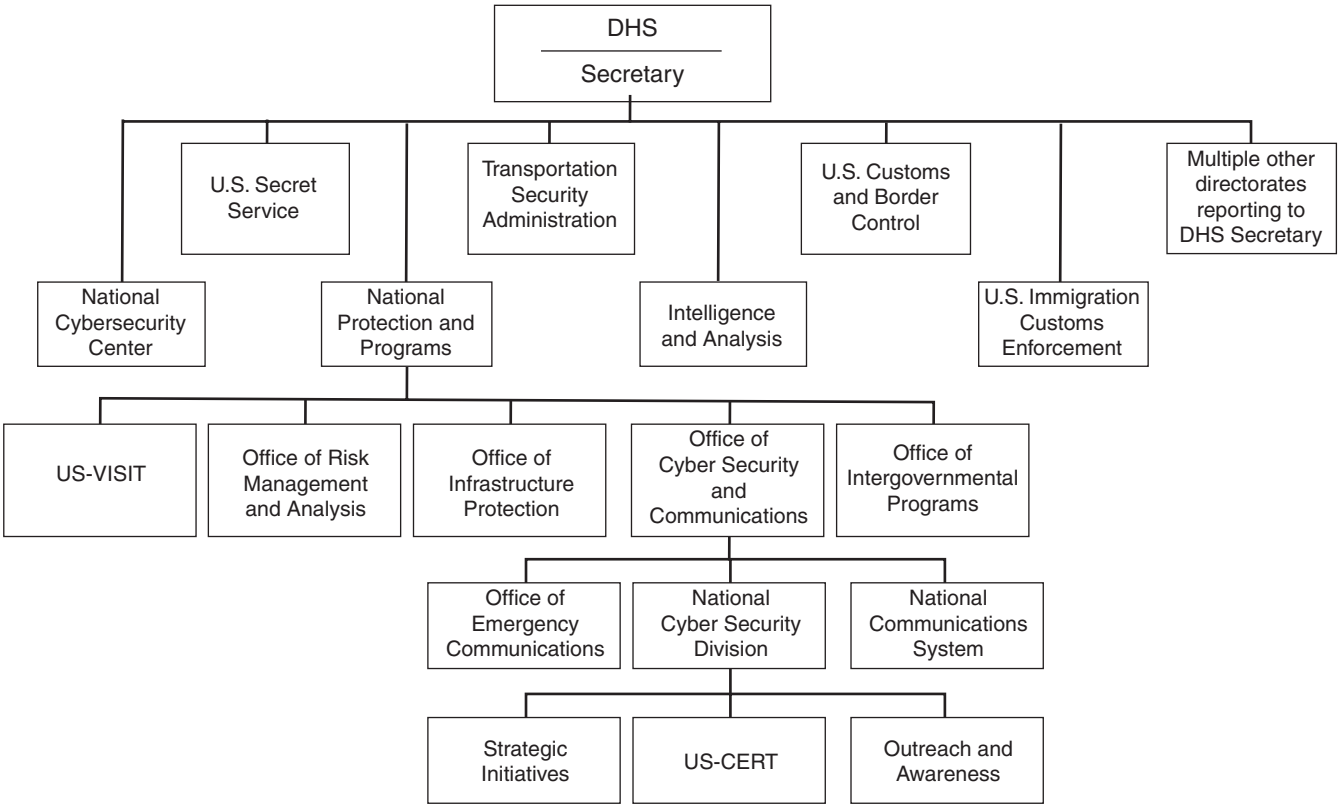
In January 2008, the President issued HSPD 23—also referred to as National Security Presidential Directive 54 and the President's "Cyber Initiative"—to improve the federal government's cybersecurity efforts, including protecting against intrusion attempts and better anticipating future threats.[16] While the directive is a classified document, US-CERT officials stated that it includes steps to enhance cyber analysis related efforts, such as requirements that federal agencies implement a centralized monitoring tool and that the federal government reduce the number of connections to the Internet, referred to as Trusted Internet Connections.

DHS Established US-CERT to Provide National Cyber Analysis and Warning

To help protect the nation's information infrastructure, DHS established the US-CERT. It is currently positioned within the NCSD of DHS's Office of Cybersecurity and Communications. Figure 1 shows the position of these offices within DHS's organizational structure.

[16]The White House, *National Security Presidential Directive 54/Homeland Security Presidential Directive 23* (Washington, D.C.: Jan. 8, 2008).

Figure 1: Department of Homeland Security Organizational Chart



Source: GAO based on DHS data.

US-CERT is to serve 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.[17] 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, the organization is to collect incident reports from all federal agencies and assist agencies in their incident response efforts. It is also to accept incident reports when voluntarily submitted by other

[17]Nonfederal entities include state and local governments, private sector entities, and individuals.

public and private entities and assist them in their response efforts, as requested.

US-CERT is composed of five branches, as shown in figure 2: Operations, Situational Awareness, Law Enforcement and Intelligence, Future Operations, and Mission Support. Each branch has specific responsibilities

- The Operations branch is to receive and respond to incidents, disseminate reasoned and actionable cybersecurity information, and analyze various types of data to improve overall understanding of current or emerging cyber threats affecting the nation's critical infrastructure.

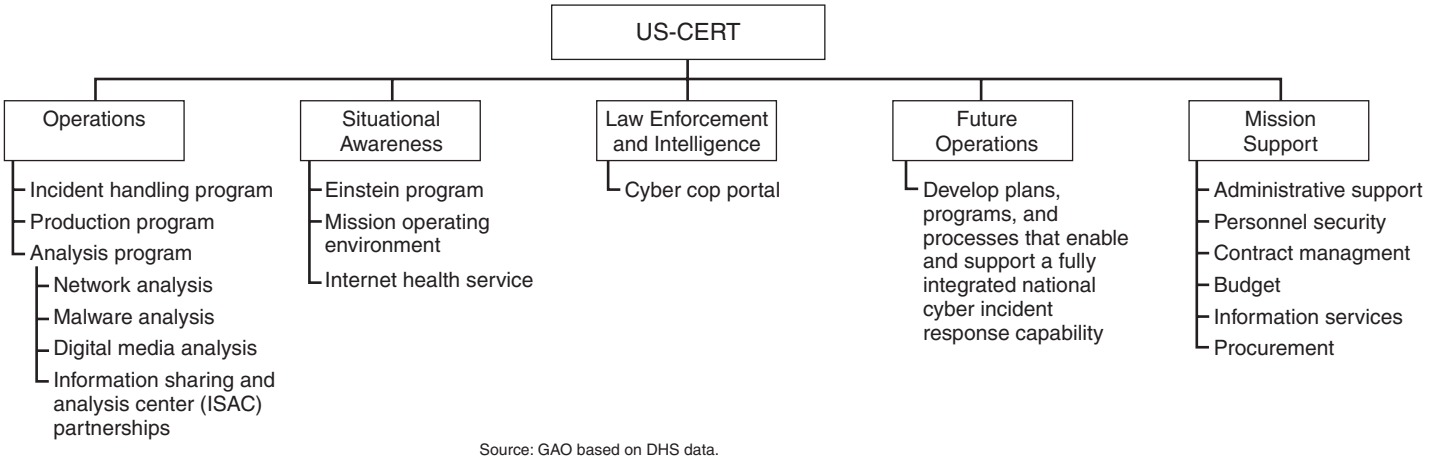
- The Situational Awareness branch is to identify, analyze, and comprehend broad network activity and to support incident handling and analysis of cybersecurity trends for federal agencies so that they may increase their own situational awareness and reduce cyber threats and vulnerabilities. As part of its responsibilities, the branch is responsible for managing the information garnered from the US-CERT Einstein program, which obtains network flow data from federal agencies, and analyzing the traffic patterns and behavior. This information is then combined with other relevant data to (1) detect potential deviations and identify how Internet activities are likely to affect federal agencies and (2) provide insight into the health of the Internet and into suspicious activities.

- The Law Enforcement and Intelligence branch is to facilitate information sharing and collaboration among law enforcement agencies, the intelligence community, and US-CERT through the presence of liaisons from those organizations at US-CERT.

- The Future Operations branch was established in January 2007 to lead or participate in the development of related policies, protocols, procedures, and plans to support US-CERT's coordination of national response to cyber incidents.

- The Mission Support branch is to manage US-CERT's communications mechanisms, including reports, alerts, notices, and its public and classified Web site content.

Figure 2: US-CERT Organizational Structure



Source: GAO based on DHS data.

Cyber Analysis and Warning Encompasses Four Key Capabilities

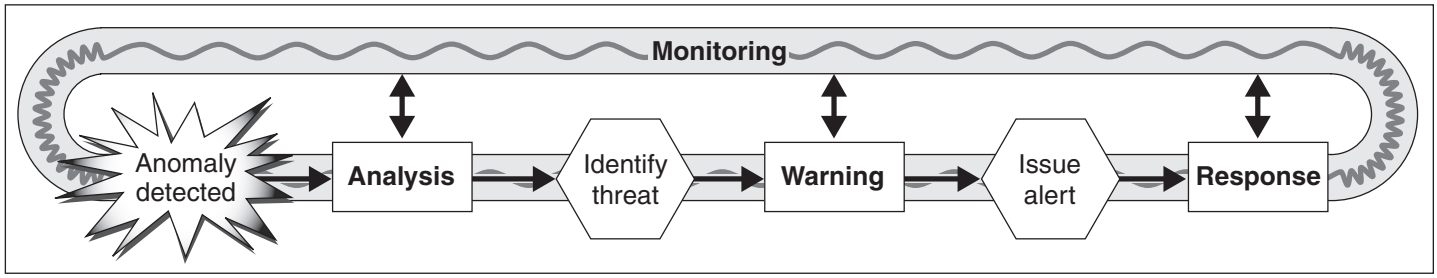
Our research and observations at federal and nonfederal entities show that cyber analysis and warning typically encompasses four key capabilities:

- **Monitoring**—detecting cyber threats, attacks, and vulnerabilities and establishing a baseline of system and communication network assets and normal traffic.
- **Analysis**—using the information or intelligence gathered from monitoring to hypothesize about what the threat might be, investigate it with technical and contextual expertise and identify the threat and its impact, and determine possible mitigation steps. Analysis may be initiated in reaction to a detected anomaly. This is a tactical approach intended to triage information during a cyber incident and help make decisions. It may also be predictive, proactively reviewing data collected during monitoring to look at cyber events and the network environment to find trends, patterns, or anomaly correlations that indicate more serious attacks or future threats.
- **Warning**—developing and issuing informal and formal notifications that alert recipients in advance of potential or imminent, as well as ongoing, cyber threats or attacks. Warnings are intended to alert entities to the presence of cyber attack, help delineate the relevance and immediacy of cyber attacks, provide information on how to remediate vulnerabilities and mitigate incidents, or make overall statements about the health and welfare of the Internet.

- **Response**—taking actions to contain an incident, manage the protection of network operations, and recover from damages when vulnerabilities are revealed or when cyber incidents occur. In addition, response includes lessons learned and cyber threat data being documented and integrated back into the capabilities to improve overall cyber analysis and warning.

Through our consultations with experts, we found that the terminology may vary, but the functions of these capabilities are fairly consistent across cyber analysis and warning entities. Figure 3 depicts the basic process of cyber analysis and warning capabilities.

Figure 3: A Simplified View of How Cyber Analysis and Warning Capabilities Are Executed



Source: GAO analysis.

Typically, cyber analysis and warning is executed, or managed, from a central focal point known as an operation center or watch center. Such centers can serve a single organization or a number of organizations. Centers generally include physically and electronically connected multidisciplinary teams with access to a variety of communication and software tools. The teams are made up of specialized analysts, sometimes referred to as watch standers, with a combination of expertise in information security, intelligence, and cyber forensics. Teams may also include subject area experts with specialized expertise in certain critical infrastructure sectors, industries, or technologies. The centers operate tools that integrate data and facilitate analysis by the watch standers. The data come from a multitude of sources, including internal or external monitoring, human or signals intelligence, analytical results, warnings from other entities, and information collected from previous threat responses. Centers decide when and how to issue formal and informal warnings that contribute to further analysis or provide information that aids in decisions about how to respond to an incident.

Depending on the size and organizational structure of an organization, the analysis and warning team may work with incident response teams during a cyber incident. The incident response team manages the decisions required for handling an incident using information discovered during monitoring, analysis, and warning. The team may also coordinate with those responsible for information security for the organization in order to assess risks, remediate vulnerabilities, and prepare for and respond to attacks.

Fifteen Key Attributes Essential to Establishing Cyber Analysis and Warning Capabilities

Our research and past experience at federal and nonfederal entities identified 15 key attributes associated with the cyber analysis and warning capabilities of monitoring, analysis, warning, and response. These attributes are displayed in table 4, which is followed by a detailed description by capability of each attribute.

Table 4: Key Attributes of the Cyber Analysis and Warning Capabilities

Capability	Attribute
Monitoring	Establish a baseline understanding of network assets and normal network traffic volume and flow
	Assess risks to network assets
	Obtain internal information on network operations via technical tools and user reports
	Obtain external information on threats, vulnerabilities, and incidents through various relationships, alerts, and other sources
	Detect anomalous activities
Analysis	Verify that an anomaly is an incident (threat of attack or actual attack)
	Investigate the incident to identify the type of cyber attack, estimate impact, and collect evidence
	Identify possible actions to mitigate the impact of the incident
	Integrate results into predictive analysis of broader implications or potential future attack
Warning	Develop attack and other notifications that are targeted and actionable
	Provide notifications in a timely manner
	Distribute notifications using appropriate communications methods
Response	Contain and mitigate the incident
	Recover from damages and remediate vulnerabilities
	Evaluate actions and incorporate lessons learned

Source: GAO analysis.

Monitoring

Monitoring provides the data used to understand one's operating environment and detect changes that indicate the presence of anomalies that may be cyber attacks. It encompasses five key attributes:

1. Establishing a baseline understanding of network assets and normal network traffic volume and flow

In order to detect unusual activity in network traffic or changes in an operating environment, organizations require knowledge of ordinary traffic and environmental conditions. This knowledge forms the baseline against which changes or anomalies can be detected, identified, and mitigated. A baseline is established through activities such as creating an accurate inventory of systems, prioritizing resources and assets, maintaining an understanding of the expected volume and nature of network traffic, and instituting operational procedures such as procedures for handling incidents. Without a baseline, it may be difficult to effectively detect threats or respond to a warning with the appropriate resources.

2. Assessing risks to network assets

Assessments should be conducted to determine what risks are posed by combinations of threats and vulnerabilities and inform the monitoring capability so that it is focused on the most critical assets. According to CERT® Coordination Center (CERT/CC) officials,[18] having a baseline knowledge of networks and systems and their associated risks in advance helps individual organizations understand what threats they may be susceptible to, what resources are at risk, and what the potential damage of an attack might be. Risks should be prioritized and mitigated until a reasonable acceptable level of risk is reached.

3. Obtain internal information on network operations via technical tools and user reports

Another key attribute is monitoring traffic on internal networks using (1) network and information security-related technology tools and (2) reports on network activity. As table 5 shows, various technologies can be used for internal network monitoring to help compile and identify patterns in

[18]The CERT Coordination Center is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by the Carnegie Mellon University. CERT Coordination Center is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

network data. Each type of technology may detect anomalies that the other types of software cannot.

Table 5: Common Types of Technology Used for Internal Monitoring

Technology	Function
Antivirus software	Provides protection against malicious code, such as viruses, worms, and Trojan horses.
Firewalls	Control access to and from a network or computer.
Intrusion detection systems	Detect inappropriate, incorrect, or anomalous activity on a network or computer system.
Intrusion prevention systems	Build on intrusion detection systems to detect attacks on a network and take action to prevent them from being successful.
Signature-based tools	Compare files or packets to a list of "signatures"—patterns of specific files or packets that have been identified as a threat. Each signature is the unique arrangement of zeros and ones that make up the file.
Security event correlation tools	Monitor and document actions on network devices and analyze the actions to determine if an attack is ongoing or has occurred. Enable an organization to determine if ongoing system activities are operating according to its security policy.
Scanners	Analyze computers or networks for security vulnerabilities.

Source: GAO.

These technologies can be used to examine data logs from networks on a 24-hour-a-day, 7-day-a-week schedule in an effort to identify (1) precursors and indicators of cyber threats or other anomalies and (2) the occurrence of known attacks. The data logged from these technologies are typically prepared using automated tools to help analysts observe or detect a single anomaly or to discover patterns in data over time. According to several federal and nonfederal entities, hands-on monitoring by trained analysts is essential because it can be difficult for automated tools to identify anomalies and incidents. For example, some automated signature-based tools focus on known threats and may not automatically recognize or alert analysts to new attack patterns or new threat delivery techniques. Other intrusion detection systems can produce large numbers of alerts indicating a problem when one does not exist (false positives); therefore, an analyst must look into anomalies more closely to see if detected intrusions are indications of a threat or simply an equipment malfunction.

4. Obtaining external information on threats, vulnerabilities, and incidents through various relationships, alerts, and other sources

External monitoring includes observing and receiving information that is either publicly or not publicly available for the purpose of maintaining

environmental or situational awareness, detecting anomalies, and providing data for analysis, warning, and response. External sources of information include

- formal relationships, such as with and between critical infrastructure sector-related information sharing and analysis centers (ISAC);[19] federal agencies, including military, civilian, law enforcement, and intelligence agencies; international computer emergency response team organizations; the CERT/CC and vendors under contract for services;
- informal relationships established on a personal basis between analysts located at different operations centers;
- alerts issued by federal, state, and local governments;
- alerts issued by commercial external sources such as network security and antivirus software vendors;
- vulnerability databases, standards, and frameworks such as the National Vulnerability Database,[20] the Common Vulnerability and Exposures List,[21]

[19]ISACs are to facilitate the private sector's participation in critical infrastructure protection efforts by serving as mechanisms for gathering and analyzing information and sharing it among the critical infrastructure sectors and between the private sector and government. ISACs have been established for many sectors, including financial services, electricity, information technology, research and education, the states, and telecommunications.

[20]According to the National Institute of Standards and Technology, the National Vulnerability Database is the U.S. government repository of standards-based vulnerability management data. These data enable automation of vulnerability management, security measurement, and compliance (e.g., to meet the requirements of the Federal Information Security Management Act). This database includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.

[21] According to MITRE, the Common Vulnerabilities and Exposures (CVE®) list is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities. CVE's common identifiers make it easier to share data across separate information security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools.

Common Vulnerability Scoring System,[22] and the Open Vulnerability Assessment Language;[23]

- media outlets, such as television news and newspapers; and
- Web sites, such as law enforcement entities' sites, known hacker and criminal sites and chat rooms, and cooperative cyber analysis and warning services.[24]

5. Detecting anomalous activities

Continuous monitoring occurs in order to detect significant changes from the baseline operations or the occurrence of an attack through an already known threat or vulnerability. It is ultimately the detection of an anomaly—observed internally or received from external information—and the recognition of its relevance that triggers analysis of the incident to begin.

Analysis

Analysis uses technical methods in combination with contextual expertise to hypothesize about the threat and associated risks concerning an anomaly and, if necessary, determine mitigation solutions. It encompasses four key attributes:

1. Verifying that an anomaly is an incident

Once an anomaly is detected, it should be verified whether it is a genuine cyber incident by determining that the data are from a trusted source and are accurate. For example, if the anomaly was identified by an internal

[22] According to NIST, the Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and impacts of IT vulnerabilities. Specifically, CVSS provides a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores.

[23] According to MITRE, Open Vulnerability and Assessment Language (OVAL™) is an international information security community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services.

[24] The SANS Internet Storm Center (ISC) is an example of a cooperative cyber analysis and warning center. The ISC provides free analysis and warning services for those who monitor the Web site. Participation is voluntary. In addition, the SANS Institute sponsors intrusion detection software that acts as a monitoring sensor for data collection from which threat information and data trends can be analyzed.

sensor, analysts start by confirming that the sensor was working correctly and not indicating a false positive. If the anomaly was reported by an external source, analysts try to determine the trustworthiness of that source and begin to identify internal and external corroborating sources. Anomalies that are verified may require in-depth investigation and incident handling or more observation through monitoring.

2. Investigating the incident to identify the type of cyber attack, estimate impacts, and collect evidence

Once the anomaly is verified as a potential, impending, or occurring incident, analysts should combine information from multiple sources and/or perform investigative testing using available tools. Analysis often occurs through collaboration between analysts, the exchange of notifications and warnings, and the use of analytical research techniques. Analysts use these techniques to investigate the type of attack, its source (where it originates), its target (whom it affects), and the immediate risk to network assets and mission performance. In addition, these techniques are used to compile evidence for law enforcement. Techniques for investigation include

- comparing and correlating additional monitoring data available with the anomaly to determine what other internal and external entities are experiencing;
- comparing data about the anomaly with standardized databases to determine if the threats are known; and
- performing investigations, such as cyber forensic examinations,[25] reverse engineering, malware analysis, and isolating anomalies in a test environment such as a honeypot or a sandbox.[26]

[25]Computer forensics is the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

[26]A honeypot is an intentionally underprotected computer host that is designed to collect data on suspicious activity. It generally has no authorized users other than its administrators. A sandbox is an isolated computer host used by analysts to let them observe cyber threats in order to gather data about how a specific threat might act. It is used to observe threats without endangering a live network and proprietary data.

3. **Identifying possible actions to mitigate the impact of the incident**

Analysis should culminate in identifying essential details about an anomaly such as what specific vulnerabilities are exploited or what impacts are expected for a specific incident. Steps should then be taken to identify alternative courses of action to mitigate the risks of the incident according to the severity of the exploit, available resources, and mission priorities. Such steps may include isolating the affected system to prevent further compromise, disabling the affected service that is being exploited, or blocking the connections providing the attacker a route into the network environment.[27] These courses of action may lead to more analysis or be used to support the warning capability.

4. **Integrating results into predictive analysis of broader implications or potential future attacks**

Information resulting from analysis of an individual incident should be used to determine any broader implications and predict and protect against future threats. This type of effort, or predictive analysis, should look beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of importance. For example, it may include detailed trend analysis of threats that have occurred over a certain period of time that is issued in public reports that discuss current trends, predict future incident activity, or emerging attack methods. However, according to many experts, this type of predictive analysis is complex and it is still difficult to predict future threats with current data.

Warning

Warnings are intended to alert entities to the presence of anomalies, help delineate the relevancy and immediacy of cyber attacks, provide information on how to remediate vulnerabilities and mitigate incidents, or make overall statements about the health and welfare of the Internet. Warning includes three key attributes:

[27]NIST, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-61 Revision 1 (Gaithersburg, Maryland: March 2008). This guide was issued to assist organizations in establishing computer security incident response capabilities and in handling incidents efficiently and effectively.

1. Developing notifications that are targeted and actionable

Warning messages should be targeted to the appropriate audience and provide details that are accurate, specific, and relevant enough to be acted upon. Developing actionable notifications requires providing the right incident information to the right person or group. If a single group is the only target of a threat, a warning directly to it may be more appropriate than a general public announcement. In addition, warnings are tailored to address technical or nontechnical recipients. Some warnings may be more appropriate for chief information officers, while other may include technical details for network administrators. Although notifications and warnings are delivered throughout incident handling, it is important to reach a balance between releasing actionable information and disclosing warnings too often, which can overwhelm the recipients and stretch limited resources. By addressing the specific audience, warnings avoid overwhelming recipients with extraneous or irrelevant information.

Also, recipients of notifications and warnings need to be able to use them to protect or defend their networks against cyber attacks. For example, many organizations have designated thresholds that determine how and when warnings are issued. To do so, the messages must include specific and accurate information about the incident as it relates to the recipient's monitoring, analysis, or response capabilities. An actionable warning may also include recommendations about how to respond to an incident. Federal and nonfederal entities also noted that sensitivity of information and privacy are key considerations when trying to develop an actionable warning. Warnings are sanitized or stripped of identifying or proprietary information in order to protect the privacy of individuals or entities involved in the incident. In addition, the federal government and its private sector partners must also adhere to procedures to make sure that they share useful information at the appropriate clearance level.

2. Providing notifications in a timely manner

Warnings are intended to give information to recipients as early as possible—preferably in advance of a cyber attack—to give them time to take appropriate action. In addition, the National Institute of Standards and Technology (NIST) provides guidance to federal agencies that describes when incidents are considered reportable and how long they may take to report them to US-CERT.[28] Similarly, several ISACs stated that

[28]NIST Special Pub. 800-61 Rev. 1.

they have procedures that determine when and how warnings are issued and when and how members should report incidents.

3. Distributing notifications using the most appropriate communications methods

Once a warning is developed, it is important to determine the best method for getting that message out without overwhelming the public or incident handlers. Warnings can be provided both informally and formally. Informal warnings between colleagues with established trusted relationships can happen quickly and without significant regard to the organizational structure. Formal warnings, which are typically held to a higher standard of accuracy by recipients than informal warnings, come in many forms, such as e-mail bulletins, vulnerability alerts, Web postings, targeted warnings to a specific entity, or broad security notices to the general public. In addition to specific formal warnings, operations centers that perform analysis and warning for multiple organizations, such as the ISACs and commercial vendors, use level-based or color-coded alert systems on their Web sites to quickly notify members and the public of the general threat status of the infrastructure or Internet. Changing from one level or color to another indicates that the threat level is increasing or decreasing. These same organizations send alerts about threats and vulnerabilities to members only or may issue specific warnings to a single organization that has been identified through analysis as being targeted by a cyber threat.

Response

Response includes actions to contain an incident, manage the protection of network operations, and recover from damages when vulnerabilities are revealed or when cyber incidents occur. It encompasses three key attributes:

1. Containing and mitigating the incident

When an incident is identified, immediate steps should be taken to protect network assets. Decisions are made to control further impacts on the network and then eliminate the threat. These actions may include installing a software patch, blocking a port known to be used by a particular threat, or deploying other appropriate network resources. In the case of a serious threat, the decision may be to turn off the network gateway and temporarily isolate the network from the Internet, depending upon what assets are at risk. One industry expert noted that investigation may occur before any mitigation steps are taken in order to consider the

necessity of law enforcement involvement. On the other hand, if little is known about a threat and it does not appear to endanger critical assets, a decision might be made to watch the threat emerge in a contained area to allow for further monitoring and analysis. Decisions to act or not are based on acceptable risks, available resources, and ability to remedy the known threat. In addition, decisions must be made in the context of the impact that actions will have on other related efforts, such as a law enforcement investigation.

2. Recovering from damage and remediating vulnerabilities

Once an incident is contained and mitigated, restoring damaged areas of the network to return it to its baseline becomes a priority. To understand the damage, a cyber damage or loss assessment may be conducted to identify, among other things, how the incident was discovered, what network(s) were affected, when the incident occurred, who attacked the network and by what methods, what was the intention of the attacker, what occurred during the attack, and what is the impact or severity of the incident. The recovery efforts may involve restoring or reinstalling computers, network devices, applications, or systems that have been compromised.

Taking action to remediate vulnerabilities in a network may also result from analysis and incident management. Entities work to discover and reduce the number of vulnerabilities in their computers, network devices, applications, or systems.

3. Evaluating actions and incorporating lessons learned

Entities should ensure that threat data, results, and lessons learned are evaluated and appropriately incorporated to improve the overall cyber analysis and warning capability. For example, teams can be used to simulate network threats by purposefully attacking a network in order to see how the network responds. From these simulations, an evaluation can be made about the response, and recommendations on how to improve can be developed. In addition, cyber simulations allow critical infrastructure organizations to prepare for threat scenarios and to test analysis, warning, and response capabilities. NIST guidance also states

that holding lessons learned meetings after major incidents is helpful in improving security measures and the incident handling process itself.[29]

US-CERT's Capabilities Include Some but Not All Aspects of Key Attributes

US-CERT has established cyber analysis and warning capabilities that include aspects of each of the key attributes. However, they do not fully incorporate all of them.

Monitoring Capability Includes Most but Not All Aspects of Key Attributes

US-CERT has established capabilities that include aspects of key attributes of monitoring. For example, it obtains internal network operation information via technical tools and Einstein; obtains external information on threats, vulnerabilities, and incidents; and detects anomalous activities based on the information it receives. However, its capabilities do not fully incorporate all of the key attributes of monitoring. For example, it has not established a baseline of our nation's critical infrastructure information systems. Table 6 shows our analysis of its monitoring capability.

[29]NIST Special Pub. 800-61, Rev. 1.

Table 6: US-CERT Capabilities Includes Most but Not All Aspects of Monitoring

Attribute	Aspects incorporated	Aspects not incorporated
Establish a baseline understanding of network assets and normal network traffic volume and flow	The organization has a limited baseline understanding of network assets and normal network traffic volume through the 16 federal participants in its situational awareness tool, US-CERT Einstein. In addition, it receives additional network flow information through contracts with information security vendors.	It does not have a comprehensive national-level baseline across the nation's computer-reliant critical infrastructure, including the information systems of federal civilian and military entities, state and local governments, the private sector, and other entities. For example, under Einstein, the organization monitors 16 agencies, a practice that does not provide an overall view of federal network traffic. In addition, the tool's current capabilities are manually driven, thereby complicating and slowing the collection and compilation of data.
Assess risks to network assets	—	Though US-CERT is involved in cyber-related risk assessment efforts being performed by other DHS organizations and the private sector, it does not perform risk assessments.
Obtain internal information on network operations via technical tools and user reports	The organization obtains internal information using security tools and user reports regarding its presence on the Internet and its internal network operations.	Its ability to obtain real-time internal traffic information is reduced by Einstein's limitation of requiring manually intensive analysis.
Obtain external information on threats, vulnerabilities, and incidents.	US-CERT monitors a variety of external information sources, including network traffic data, incident reports, and threat reports from federal, state, local, and foreign governments and the private sector, such as the following: • federal agencies providing an enhanced view of their networks through participation in Einstein; • various vendors providing Internet operational data; • the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC),[a] law enforcement, and the intelligence community, providing threat information and other data; • federal agencies reporting information security incidents to the organization, as required by the Federal Information Security Management Act;[b] • nonfederal entities voluntarily reporting incidents, malware, and other information; • foreign governments providing information on cyber incidents; • CERT/CC providing vulnerability information; and • other analysis and warning entities, including the Financial Services-ISAC, Multistate ISAC, the Internet Storm Center, and information security vendors, sharing incident and other situational awareness information.	Its information does not encompass all critical infrastructure information networks. For example, by monitoring only 16 agencies, Einstein does not provide an overall view of federal network traffic. Also, the Department of Energy and DOD use their own similar situational awareness tools, but their data are not currently combined with Einstein's data to provide a more complete view of federal traffic. There are efforts under way to develop automated information exchanges between DOD's system and Einstein, but as of March 2008, this had not been finalized. Regarding nonfederal entities, the organization does not directly monitor any private sector networks, nor are nonfederal entities required to report to it incidents or anomalous activity. Typically, nonfederal entities, including the ISACs, that report incident and other data filter sensitive details from the data reported.

Attribute	Aspects incorporated	Aspects not incorporated
Detect anomalous activities.	The organization detects anomalies based on its monitoring of network traffic flow. Einstein provides network flow data from 16 agencies with the primary goal of looking for unique activity that may indicate a cyber attack or other undesirable activity.[c] According to US-CERT officials, Einstein provides the participating agencies a capability to compare their network traffic data with activity at other federal agencies and against law enforcement and intelligence agencies' threat data to determine if they are the victim of serious attacks. In addition, it works with its various partners in the private sector as well as other federal, state, and local governments to determine the extent of abnormal behavior. For example, the organization receives limited information from certain computer security vendors regarding Internet traffic flow of their respective customer bases.	The organization does not detect anomalies across the nation's computer-reliant critical infrastructure. For example, it does not directly monitor any private sector networks, nor are nonfederal entities required to report incidents or anomalous activity.

Source: GAO analysis.

[a]HITRAC is a fusion center of intelligence analysts from DHS's Office of Intelligence and Analysis and subject matter experts from the National Protection and Programs Directorate working together to analyze threats, vulnerabilities, and risks to the 18 Critical Infrastructure/Key Resource sectors of the United States. Additionally, HITRAC focuses solely on analyzing and identifying the threat aspect of cybersecurity incidents as they occur. HITRAC shares these threat data with numerous customers, including US-CERT.

[b]The Federal Information Security Management Act requires the operation of a central federal information security incident center. 44 U.S.C. 3546. The act also requires agencies to report incidents to the organization, in addition to law enforcement agencies, relevant offices of inspector general, and other designated entities. 44 U.S.C. 3544(b)(7).

[c]These data are analyzed for traffic patterns and behavior; this information can be combined with other relevant data to (1) detect potential deviations and identify how Internet activities are likely to affect federal agencies and (2) provide insight into the health of the Internet and suspicious activities.

As part of the President's Cyber Initiative, DHS has a lead role for several provisions that, if implemented appropriately, could address key monitoring deficiencies, such as not having a comprehensive national baseline and sufficient external information on threats, vulnerabilities, and incidents. According to testimony by the Under Secretary for the National Protection and Programs Directorate, the initiative makes the Einstein program mandatory across all federal agencies. In addition, DHS plans to enhance Einstein's capabilities to be a real-time intrusion detection and situational awareness system. Further, DHS, along with the Office of Management and Budget (OMB), is responsible for working with federal agencies to reduce the number of Trusted Internet Connections used by the federal government. According to DHS and OMB officials, these initiatives will enhance the ability of the US-CERT to monitor federal systems for cyber attacks and other threats. According to US-CERT officials, the reduction in Trusted Internet Connections, along with the

positioning of Einstein in front of those connections to the Internet, will help provide a governmentwide baseline and view of the traffic entering and leaving federal networks as well as access to the content of the traffic. In addition, according to the Assistant Secretary for Cybersecurity and Communications, the recently announced National Cybersecurity Center, which reports directly to the Secretary of Homeland Security, will be responsible for ensuring coordination among the cyber-related efforts across the federal government, including improving the sharing of incident and threat information. However, the efforts to use Einstein, reduce Internet connections, and implement the National Cybersecurity Center are in their early stages and have not yet been fully planned or implemented, so whether these efforts will fully address all five of the monitoring attributes is not known at this time.

Analysis Capability Does Not Fully Incorporate All Aspects of Key Attributes

US-CERT has established capabilities that include key attributes of analysis. For example, it verifies anomalies, performs investigations, and identifies possible courses of action. However, its capabilities do not fully incorporate other attributes because of technical and human resource constraints and the gaps in the monitoring capability. Table 8 shows our analysis of the organization's analysis capability.

Table 7: US-CERT Incorporates Some but Not All Aspects of Analysis

Attribute	Aspects incorporated	Aspects not incorporated
Verify that an anomaly is an incident (threat of attack or actual attack)	When an anomaly is detected or reported, US-CERT works directly with its various public and private sector partners to determine whether the anomaly is an incident. For example, it notifies federal agencies when it observes abnormal activities. In turn, federal agencies take the information provided and are to verify whether the activity constitutes a cybersecurity incident and if any support is required from US-CERT.	The lack of a robust monitoring capability negatively affects the organization's ability to verify and investigate anomalies and to identify threats. Specifically, although the Einstein flow data are collected in real time, the actual analysis is manually intensive and does not occur simultaneously or in real time. Another limiting factor of Einstein data is that the organization is unable to analyze the content of the potentially malicious traffic.
Investigate the incident to identify the type of cyber attack, estimate impacts, and collect evidence	The organization investigates incidents through network and malware analysis. For example, it correlates Einstein network traffic data with known vulnerabilities and threats to identify abnormal activity, and then it focuses on identifying emerging threats, ongoing trends, and intrusions that have already occurred. According to agency officials, through the implementation of Einstein, the amount of time needed to discover and understand a potential cyber attack and communicate it to agencies has been significantly reduced from 4 to 5 days to 4 to 5 hours. In addition, according to US-CERT officials, its malware analysis focuses on reverse engineering malicious code to determine how the code works, its effect on a network or system, and potentially who developed it. The organization receives the malware code from a variety of sources, including its own monitoring, anonymous submissions, and formal submissions from affected entities, such as federal agencies, Internet service providers, and other entities. For example, according to agency officials, they receive on average between 5,000 and 24,000 individual pieces of malware in a 24-hour period. Additionally as of April 2008, officials stated that the organization had conducted analysis on 1,520,022 samples of malware code during fiscal year 2008. To do this work, the organization has established a segregated facility, or malware laboratory, that provides a controlled environment to conduct detailed analysis on infected computer hardware and software. According to officials, its malware capability has provided value to federal and nonfederal partners because it can analyze the potential impact of malware with the known threat information received from its partners in the law enforcement and intelligence communities.	The number of incidents that can be analyzed at one time is limited.

Attribute	Aspects incorporated	Aspects not incorporated
Identify possible actions to mitigate the impact of the incident	US-CERT's analysts develop alternative actions for stopping or controlling the threat. These alternatives are based on risk, required resources, mission priorities, and existing network requirements and limitations. Its network analysts work with all US-CERT partners to identify possible courses of action and methods to respond to cyber incidents. For example, in January 2008, an analysis of malware discovered at a targeted federal agency led to the identification of three zero-day exploits and a subsequent alert issued to federal and nonfederal entities.	The organization's ability to develop possible actions to mitigate the identified threat is limited by its inability to engage other partners in analysis efforts because the information may be sensitive or classified.
Integrate results into predictive analysis of broader implications or potential future attack	According to NCSD officials, the organization is engaged in activities with other NCSD entities to develop more strategic views of the nation's critical cyber infrastructures.	The organization does not possess the capability to integrate its work into predictive analysis.

Source: GAO analysis.

As part of the Cyber Initiative, the organization has received additional resources to develop the next version of the Einstein situational awareness tool. According to US-CERT officials, this new version, referred to as Einstein 2.0, will provide real-time intrusion detection monitoring, a content analysis capability, and automated analysis functions that are currently manual. In addition, it has received authorization for an additional 30 government and 50 contractor employee full-time equivalents. According to US-CERT officials, they plan to fill the additional positions by leveraging graduates of the Scholarship for Service program, which provides cybersecurity-related scholarships to students willing to serve the federal government for a time commitment. However, these efforts are in their early stages and have not yet been fully planned or implemented. Consequently, whether these efforts will fully address all four of the analysis attributes is not known at this time.

Warning Capability Exhibits Some but Not All Characteristics of Key Attributes

The organization has established capabilities that include key attributes of warning. For example, it develops and distributes a number of attack and other notifications targeted to different audiences with varying frequency. However, according to customers, these warning products are not consistently actionable and timely. Table 8 shows our analysis of the organization's warning capability. Tables 9 and 10 show types of warning products and the quantity of products issued during fiscal year 2007.

Table 8: US-CERT Exhibits Some but Not All Aspects of Warning

Attribute	Aspects incorporated	Aspects not incorporated
Develop attack and other notifications that are targeted and actionable	As tables 9 and 10 depict, the organization develops various attack and other notifications for a varied set of customers.	Officials from entities with robust cyber analysis and warning capabilities, such as the ISACs, DOD, and the Department of Energy, stated that the organization's notifications typically did not offer new or additional information beyond their own efforts.
Provide notifications in a timely manner	The organization is occasionally able to provide notifications to certain customers in a timely manner. For example, officials from organizations with limited cyber analysis and warning capabilities stated that certain US-CERT notifications, especially those warnings with For Official Use Only (FOUO) information, were extremely timely.	The organization is not consistently able to provide notifications in a timely manner. Its ability to disseminate timely notifications is hindered by a number of factors. First, as the national cyber analysis and warning organization, it must ensure a high level of accuracy in the products it releases. In order to avoid disseminating incomplete or inaccurate information, its warning products are subjected to a review process, which can prevent their rapid dissemination. Further, the sensitivity of information can be a hindrance. Specifically, highly sensitive information must be coordinated with other components as part of the review process, which can add days to the release time. Finally, dissemination efforts are limited by lack of performance measures that assess or provide feedback on the value of US-CERT products.
Distribute notifications using appropriate communications methods	As table 9 depicts, the organization distributes a wide array of attack and other "warning" products through various mechanisms to a diverse set of customers.	According to NSCD officials, the organization is refining its distribution lists and collaborating with various federal and nonfederal user groups to better ensure appropriate officials (those having the understanding and ability to appropriately respond) receive its notifications.

Source: GAO analysis.

(This page left blank intentionally)

Table 9: US-CERT Warning Products, Fiscal Year 2007

	Product audience					
US-CERT products	**White House**	**Federal government**	**GFIRST[a]**	**Select international partners[b]**	**ISACs[c]**	**General public**
Situational awareness report	●		●	●	●	
Federal information notice	●	●	●			
Critical infrastructure information notice	●			●	●	
Public trends and analysis report		●	●	●	●	●
Technical information paper	●	●	●	●	●	●
Cyber daily briefing			●		●	
Non-technical alerts						●
Technical alerts	●	●	●	●	●	●
Security bulletins	●	●	●	●	●	●
Security tips						●
Current activity	●	●	●	●	●	●
Vulnerability notes	●	●	●	●	●	●

Distribution mechanism						Frequency					
US-CERT Web site	US-CERT HSDN Web site[d]	US-CERT HSIN portal[e]	NCAS[f]	E-mail distribution	RSS feeds[g]	Daily	Weekly	Every other week	Monthly	Quarterly	As needed
	●	●							●		●
	●	●		●							●
	●	●		●							●
●	●	●								●	
●	●	●									●
		●		●		●					
●	●		●	●							●
●	●		●	●	●		●				●
●	●		●	●	●		●				
●			●	●	●			●			
●	●			●	●	●					●
●	●			●	●						●

Source: US-CERT

[a]Government Forum of Incident Response and Security Teams (GFIRST) is a group of technical and tactical practitioners from government agency security response teams responsible for securing government information technology systems.

[b]Select international partners including Australia, Canada, New Zealand, and the United Kingdom.

[c]Information sharing and analysis center.

[d]Homeland Secure Data Network (HSDN) is a secure portal that provides the ability to share information at the Secret category level among other federal, state, and local government entities.

[e]DHS considers the Homeland Security Information Network (HSIN) to be its primary communication application for transmitting sensitive but unclassified information. According to DHS, this network is an encrypted, unclassified, Web-based communications application that serves as DHS's primary nationwide information-sharing and collaboration tool. It is intended to offer both real-time chat and instant messaging capability, as well as a document library that contains reports from multiple federal, state, and local sources.

[f]DHS established the National Cyber Alert System (NCAS) to deliver targeted, timely, and actionable information to the public on how to secure computer systems. Information provided by the alert system is designed to be understandable by all computer users, both technical and nontechnical.

[g]Really Simple Syndication (RSS) is a format for gathering and making available content from Web sites. RSS can be used to provide any kind of information that can be broken down into discrete items and put into RSS format, typically called an RSS feed. Software is available that can periodically check RSS feeds for changes, download new items, and make them available to the users.

Table 10: Quantity of US-CERT Warning Products, Fiscal Year 2007

Product	Quantity	Interval
Public trends and analysis reports	4	Quarterly
Vulnerability notes	353	As needed
Situational awareness reports (SAR)	83	As needed
Federal information notices (FIN)	7	As needed
Technical information papers (TIP)	8	As needed
Critical infrastructure information notices (CIIN)	9	As needed
Security bulletins	52	Weekly
Technical alerts	39	As needed
Nontechnical alerts	27	As needed
Current activity	260	As needed
Cyber daily briefings	356	Daily

Source: US-CERT.

As part of the Cyber Initiative, the enhancements to the Einstein program, as well as the reduction in the number of Trusted Internet Connections can lead to more complete data. According to US-CERT officials, the improved data will lead to an enhanced warning capability that could provide the ability to issue targeted and actionable alerts in advance of actual cyber attacks. However, these efforts are in their early stages and have not yet been fully planned or implemented; thus, it is not clear whether these efforts will fully address the three warning attributes.

Response Capability Satisfies Some but Not All Aspects of Key Attributes

US-CERT possesses a limited response capability to assist other entities in the containment, mitigation, and recovery from significant cyber incidents. For example, while it provides on-site assistance to various entities, its ability to provide response at the national level is hindered by limitations in the resources available and authority over affected entities. Table 11 shows our analysis of its response capability.

Table 11: US-CERT Satisfies Some but Not All Aspects of Response

Attribute	Aspects incorporated	Aspects not incorporated
Contain and mitigate the incident	The organization assists entities in federal, state, and local governments as well as the private sector with the containment and mitigation of cybersecurity incidents as they occur, on a requested basis. According to agency officials, the US-CERT routinely deploys its two digital media analysis teams to perform on-site response to serious incidents. These teams have the capabilities and depth of knowledge to perform detailed analysis on compromised media (e.g., hard drives and thumb drives). For example, as of April 2008, the organization had provided on-site incident response eight times for fiscal year 2008, making about 30 visits to various federal agencies to address incidents dealing with unauthorized access, malware activity, as well as misconfigured network devices. Also, in November 2007, the organization deployed at least one response team to each of five different federal agencies over 5 consecutive days. In addition, the Law Enforcement and Intelligence branch works with organizations such as the Federal Bureau of Investigation and United States Secret Service to contain incidents on a global scale using established relationships with other nations. According to officials, the organization has also assisted at the international level, most recently deploying officials to Estonia to help its government improve its cybersecurity posture after suffering a major cyber attack. Further, DHS, in conjunction with DOD and the Department of Justice, formed the NCRCG to coordinate the federal response to cyber incidents of national significance. During a significant national incident, the NCRCG is to provide subject matter expertise, recommendations, and strategic policy support to the Secretary of Homeland Security. At the time of our review, the senior-level membership had coordinated and communicated about incidents; however, there had not been a cyber incident of national significance to activate these procedures.	Though the organization is responsible for responding to national-level incidents, it does not possess the authority to compel an agency or organization to take action.
Recover from damages and remediate vulnerabilities	The organization routinely deploys its two digital media analysis teams to perform on-site response to serious incidents at federal agencies. According to agency officials, these teams focus on serious incidents, typically involving advanced threats, such as those propagated by nation states as well as advanced malware attacks.	To handle a cyber attack that affects multiple entities across the nation, officials stated that the organization would need at least three additional digital media analysis teams.

Attribute	Aspects incorporated	Aspects not incorporated
Evaluate actions and incorporate lessons learned	US-CERT has identified shortcomings in its processes, communications methods, and policies by conducting exercises that simulate a national-level incident. For example, once a digital media team has completed its on-site response assistance, it generates an after-action report that summarizes what steps were taken and any further suggested actions for the affected organization. In addition, during Cyber Storm II, which occurred in March 2008, the organization identified a number of issues for improvement that will be addressed in after-action reports and tracked to ensure changes occur.	While it measures certain items, such as the number and type of products it distributes, the organization has not established performance measures to determine the effectiveness of its efforts. According to US-CERT officials, other than an occasional statement of appreciation from other organizations, they do not know who benefits from their efforts or who uses their products.

Source: GAO analysis.

To improve the organization's response capability, US-CERT officials stated that they needed to perform internal exercises that test its national-level response capability more often than every 2 years, as is the case with the Cyber Storm exercise.[1] It plans to develop "tabletop" exercises to more frequently test its response capabilities. In addition, according to NCSD officials, they are working collaboratively with other federal and nonfederal working groups to improve their performance measures so that they can understand the value and use of their products and make continuous improvements. However, until they do so, it is not clear whether these efforts will lead to US-CERT fully addressing the three response attributes.

US-CERT Faces New and Ongoing Challenges to Fulfilling Its Mission

US-CERT faces a number of newly identified and ongoing challenges that impede it from fully implementing the key attributes and in turn establishing cyber analysis and warning capabilities essential to coordinating the national effort to prepare for, prevent, and respond to cyber threats. The new challenge is creating warnings that are actionable and timely—it does not consistently issue warning and other notifications that its customers find useful. In addition, US-CERT continues to face four challenges that we previously identified: (1) employing predictive cyber analysis, (2) developing more trusted relationships to encourage information sharing, (3) having sufficient analytical and technical capabilities, and (4) operating without organizational stability and

[1]Cyber Storm is a biennial national-level exercise to test the ability of federal and nonfederal stakeholders, including federal, state, and local agencies; private sector entities; and foreign governments, to respond to major cyber attacks. The last exercise, referred to as Cyber Storm II, was held in March 2008.

leadership within DHS. Until DHS addresses these challenges and fully incorporates all key attributes into its capabilities, it will not have the full complement of cyber analysis and warning capabilities essential to effectively performing its national mission.

New Challenge Involves Creating Warnings That Are Actionable and Timely

Developing and disseminating cyber threat warnings to enable customers to effectively mitigate a threat in advance of an attack can be challenging for the US-CERT. According to the organization's Acting Deputy Director, it serves as the nation's cyber analysis and warning center and must ensure that its warnings are accurate. In addition, owners of classified or law enforcement information must review and agree to the release of related information. Therefore, the organization's products are subjected to a stringent review and revision process that could adversely affect the timeliness of its products—potentially adding days to the release if classified or law enforcement information must be removed from the product. For example, an official from a cybersecurity-focused organization at a university stated that the alerts from US-CERT generally arrive a day or two after they might have been helpful. An official from another private entity stated that the bureaucratic process US-CERT must follow prevents it from providing useful alerts in a timely manner and that as a result, it does not have the credibility to drive a reaction when an alert is finally issued. Another private sector official stated that, in some cases, the organization gets information on cyber incidents and attacks faster from media sources than US-CERT because its analysts need time to verify the reliability of the data they receive.

In addition, according to federal officials responsible for determining cyber-related threats, US-CERT, as well as other organizations with cybersecurity-related responsibilities, must also balance the need to develop and release warnings with the activities of other organizations, such as law enforcement and intelligence support, to identify and mitigate cyber threats. For example, the release of a warning to address a threat or attack may also alert the intruders that their methods have been discovered and cause them to change their methods prior to the completion of an investigation about their activities.

Further, when there is sensitive information to share, US-CERT officials stated that on numerous occasions, they were unable to share the details of threats to customers' networks because no one within the federal agency or nonfederal entity possessed a security clearance high enough to receive the information. In some organizations, the individuals who do possess security clearances are in the upper echelons of the organization

and do not possess a cyber or information security background. As a result, they are not always able to accurately comprehend and relay the threat information to those who would actually handle the mitigation efforts. In September 2007, we reported that DHS lacked a rapid, efficient process for disseminating sensitive information to private industry owners and operators of critical infrastructures.[2] We recommended that DHS establish a rapid and secure process for sharing sensitive vulnerability information with critical infrastructure stakeholders, including vendors, owners, and operators; however, DHS has not yet fulfilled this recommendation.

To provide actionable information to its customers, the organization attempts to combine incident information with related cyber threat information to determine the seriousness of the attack. However, according to the Acting Director of US-CERT, its efforts are limited by other federal entities' abilities to determine specific cyber threats to the nation's critical infrastructure. One reason for the lack of cyber threat data is that the task is complex and difficult and there are no established, generally accepted methodologies for performing such analysis. In addition, such entities are hampered by the limited number of analysts dedicated to cyber threat identification. For example, in January 2008, the Director of HITRAC stated that only 5 percent of HITRAC's total number of analyst positions was focused on analyzing and identifying cyber threats to our nation's critical information infrastructure. According to the director, it had received approval to double the number of cyber-related analysts and was in the process of filling those positions. In addition, the director stated that HITRAC's primary focus is on identifying physical threats.

Ongoing Challenges Involve Establishing Predictive Analysis, Trusted Relationships, Analytical and Technical Capabilities, and a Stable Organization

US-CERT faces ongoing challenges that we identified in previous reports as impeding DHS's ability to fulfill its cyber critical infrastructure protection responsibilities.

Employing predictive cyber analysis—US-CERT has been unable to establish the solid foundation needed to perform predictive cyber analysis that would enable it to determine any broader implications from ongoing network activity, predict or protect against future threats, or identify emerging attack methods prior to an attack. Since 2001, we have identified

[2]GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007).

the challenges associated with establishing strategic, predictive analysis and warning and have made recommendations that responsible executive branch officials and agencies establish such capabilities, including developing methodologies.[3] According to the Acting Director of US-CERT, it has not been able to establish such capabilities because there is not a generally accepted methodology for performing predictive cyber analysis and warning. In addition, officials from US-CERT and other federal and nonfederal entities with cyber analysis and warning capabilities stated that while they can determine the motivations for the various threat sources to use cyber attacks, it is a formidable task to foresee prior to attacks how those threats would actually conduct attacks and to establish indicators to recognize that such cyber attacks are about to occur. Also, the relative newness of the cyber analysis and warning discipline and immaturity of the related methodologies and tools add to the complexity.

Developing more trusted relationships to encourage information sharing—Implementing cyber analysis and warning capabilities, including all of the key attributes, requires that entities be willing and able to share information, including details about incidents, threats, vulnerabilities, and network operations. However, US-CERT continues to be challenged to develop relationships with external sources that would encourage information sharing. For example, nonfederal entities do not consistently fully disclose incident and other data—they filter sensitive details from the data reported, thus reducing its value to US-CERT. The lack of such relationships negatively affects the organization's cyber analysis and warning capability.

In 2005, we reported that entities within critical infrastructure sectors possess an inherent disincentive to share cybersecurity information with DHS.[4] Much of their concern was that the potential release of sensitive information could increase the threat they face. In addition, when information was shared, it was not clear whether the information would be shared with other entities, such as other federal entities, state and local entities, law enforcement, or various regulators, or how it would be used or protected from disclosure. Alternatively, sector representatives expressed concerns that DHS was not effectively communicating information with them and had not matched private sector efforts to share valuable information with a corresponding level of trusted information

[3]GAO-01-323.

[4]GAO-05-434.

sharing. We also identified information sharing in support of homeland security as a high-risk area in 2005, and we noted that establishing an effective two-way exchange of information to help detect, prevent, and mitigate potential terrorist attacks requires an extraordinary level of cooperation and perseverance among federal, state, and local governments and the private sector.[5]

Federal and nonfederal officials raised similar concerns about the ability to develop trusted relationships and share information with and between cyber analysis and warning entities, including US-CERT. For example, frequent staff turnover at NCSD and US-CERT hindered the ability to build trusted relationships with both public and private entities. Federal and nonfederal officials stated that reliance was placed on personal relationships to support sharing of sensitive information about cybersecurity and cyber incidents. However, according to the NCSD director, six senior staff members within the Office of Cybersecurity and Communications (the national focal point for addressing cybersecurity issues) were leaving for various reasons, affecting the ability to develop such relationships. In addition, private sector officials stated that their organizations continued to be hesitant to share information on vulnerabilities and threats because of the fear that such sharing might negatively affect their financial bottom line. For example, private sector officials stated that it was difficult to share unfiltered information with their respective infrastructure sector ISAC because a competitor operated the ISAC, thus negatively affecting the information received by US-CERT.

Having sufficient analytical and technical capabilities—Obtaining and retaining adequately trained cyber analysts and acquiring up-to-date technological tools to implement the analysis capability attributes is an ongoing challenge to US-CERT and other analysis and warning centers, hindering their ability to respond to increasingly fast, nimble, and sophisticated cyber attacks. As we have reported, NCSD has had difficulty hiring personnel to fill vacant positions.[6] We reported that once it found qualified candidates, some candidates decided not to apply or withdrew their applications because it took too long to be hired. This is still a concern because current staff has limited organizational backup and, in some cases, performs multiple roles. In addition, a private sector official stated that it is not clear whether or not the government has the number of

[5]GAO-05-207.

[6]GAO-05-434.

technical analysts necessary to perform analysis on large and complex data sets that are generated whether or not an incident is in progress or not.

Keeping cyber analysts trained and up to date on the latest cybersecurity tools and techniques can be difficult. For example, a DOD official representing one of its cyber analysis and warning centers stated that its analysts must develop their expertise on the job because there is no formal training program available that teaches them how to detect and perform analysis of an anomaly or intrusion. A private sector official stated that while analysts are often trained to use existing tools, their understanding of the key attributes of analysis is often limited, resulting in a solution too late to be helpful.

Analysts also need the appropriate technological tools to handle the volume, velocity, and variety of malicious data and activity they are faced with, according to federal officials. For example, although the Einstein flow data are collected in real time, the actual analysis is manually intensive and does not occur simultaneously or in real time. Another limiting factor of Einstein data is that US-CERT is unable to analyze the content of the potentially malicious traffic and must rely on the affected agency to perform any analysis of the content of the traffic. Thus both the reaction time to determine the intent of the anomalous activity and the necessary actions to address it are significantly slowed. In addition, officials from one private sector entity questioned if agencies can sufficiently protect their networks using the tools they are mandated to use.

As part of the efforts to address the President's Cyber Initiative, US-CERT recently received approval to fill 80 new positions—30 government and 50 contractor—and is attempting to fill these analytical positions by extending offers to candidates in the National Science Foundation's Scholarship for Service Program. However, these positions have yet to be completely filled with qualified candidates.

Operating without organizational stability and authority—We have identified challenges regarding DHS's organizational stability, leadership, and authority that affect US-CERT's ability to successfully perform its mission. In the past, we have reported that the lack of stable leadership has diminished NCSD's ability to maintain trusted relationships with its

infrastructure partners and has hindered its ability to adequately plan and execute activities.[7] While DHS has taken steps to fill key positions, organizational instability among cybersecurity officials continues to affect NCSD and thus US-CERT. For example, at least six senior staff members were leaving DHS's Office of Cybersecurity and Communications, including the NCSD Director. Losing senior staff members in such large numbers has negatively affected the agency's long-term planning and hampered the ability of NCSD/US-CERT to establish trusted relationships with public and private entities and to build adequate functions to carry out its mission, including expanded cyber analysis and warning capabilities, according to the official.

Furthermore, when new senior leadership has joined DHS, NCSD/US-CERT's objectives were reassessed and redirected, thus affecting NCSD's ability to have a consistent long-term strategy, according to the former official. For example, senior officials wanted to broaden the role and focus of US-CERT by having it provide centralized network monitoring for the entire federal government on a 24-hour-a-day, 7-day-a-week basis. However, the Director of NCSD disagreed with this strategy, stating that each federal agency should have its own 24-hour-a-day, 7-day-a-week incident-handling capability (either in-house or contracted out) to respond to incidents affecting its own network. He viewed US-CERT as a fusion center that would provide analysis and warning for national-level incidents, support federal agency incident-handling capabilities during crisis situations, and offer a mechanism for federal agencies to coordinate with law enforcement.

The organization's future position in the government's efforts to establish a national-level cyber analysis and warning capability is uncertain. Specifically, Homeland Security Presidential Directive 23, which is classified, creates questions about US-CERT's future role as the focal point for national cyber analysis and warning. In addition, DHS established a new National Cybersecurity Center at a higher organizational level, which may diminish the Assistant Secretary of Cyber Security and Communications' authority as the focal point for the federal government's cybersecurity-related critical infrastructure protection efforts, and thus US-CERT's role as the central provider of cyber analysis and warning capabilities across federal and nonfederal critical infrastructure entities.

[7] GAO-05-434.

As stated above, we did not make new recommendations in 2005 regarding cyber analysis and warning because our previous recommendations had not yet been fully implemented. At the time, we did recommend that the Secretary of Homeland Security require NCSD to develop a prioritized list of key activities for addressing the underlying challenges related to information sharing, hiring staff with appropriate capabilities, and organizational stability and authority. In addition, we recommended that performance measures and milestones for performing activities to address these challenges be identified. However, since that time, DHS has not provided evidence that it has taken actions on these activities.

Conclusions

In seeking to counter the growing cyber threats to the nation's critical infrastructures, DHS has established a range of cyber analysis and warning capabilities, such as monitoring federal Internet traffic and the issuance of routine warnings to federal and nonfederal customers. However, while DHS has actions under way aimed at helping US-CERT better fulfill attributes identified as critical to demonstrating a capability, US-CERT still does not exhibit aspects of the attributes essential to having a truly national capability. It lacks a comprehensive baseline understanding of the nation's critical information infrastructure operations, does not monitor all critical infrastructure information systems, does not consistently provide actionable and timely warnings, and lacks the capacity to assist in mitigation and recovery in the event of multiple, simultaneous incidents of national significance.

Planned actions could help to mitigate deficiencies. For example, as part of the Cyber Initiative, US-CERT plans to enhance its Einstein situational awareness tool so that it has real-time intrusion detection monitoring, a content analysis capability, and automated analysis functions. By placing the tool in front of Trusted Internet Connections, officials expect to obtain a governmentwide baseline view of the traffic and content entering and leaving federal networks. US-CERT also plans to hire 80 additional cyber analysts and to increase the frequency of exercises that test its national-level response capability.

However, at this point, it is unclear whether these actions will help US-CERT—or whatever organizational structure is ultimately charged with coordinating national cyber analysis and warning efforts—achieve the objectives set forth in policy. DHS faces a number of challenges that impede its ability to achieve its objectives, including fostering trusted relationships with critical infrastructure sectors, hiring and retaining skilled cyber analysts, ensuring that US-CERT warning products provide

useful information in advance of attacks, enhancing predictive analysis, and ensuring that any changes brought about by HSPD 23 are marked by well-defined and transparent lines of authority and responsibility. We identified most of these challenges in our prior reviews and made broad recommendations to address them. DHS's actions to address these challenges have not been adequate. Because of this, addressing these challenges is as critical as ever to overcome the growing and formidable threats against our nation's critical cyber infrastructure. If these challenges are not addressed, US-CERT will not be able to provide an effective national cyber analysis and warning capability.

Recommendations for Executive Action

We recommend that the Secretary of Homeland Security take four actions to fully establish a national cyber analysis and warning capability. Specifically, the Secretary should address deficiencies in each of the attributes identified for

- monitoring, including establish a comprehensive baseline understanding of the nation's critical information infrastructure and engage appropriate nonfederal stakeholders to support a national-level cyber monitoring capability;
- analysis, including expanding its capabilities to investigate incidents;
- warning, including ensuring consistent notifications that are targeted, actionable, and timely; and
- response, including ensuring that US-CERT provides assistance in the mitigation of and recovery from simultaneous severe incidents, including incidents of national significance.

We also recommend that the Secretary address the challenges that impede DHS from fully implementing the key attributes, including the following 6 items:

- engaging appropriate stakeholders in federal and nonfederal entities to determine ways to develop closer working and more trusted relationships;
- expeditiously hiring sufficiently trained cyber analysts and developing strategies for hiring and retaining highly qualified cyber analysts;
- identifying and acquiring technological tools to strengthen cyber analytical capabilities and handling the steadily increasing workload;

- developing predictive analysis capabilities by defining terminology, methodologies, and indicators, and engaging appropriate stakeholders in other federal and nonfederal entities;
- filling key management positions and developing strategies for hiring and retaining those officials; and
- ensuring that there are distinct and transparent lines of authority and responsibility assigned to DHS organizations with cybersecurity roles and responsibilities, including the Office of Cybersecurity and Communications and the National Cybersecurity Center.

Agency Comments and Our Evaluation

In written comments on a draft of this report (see app. II), signed by the Director of DHS's GAO/OIG Liaison Office, the department concurred with 9 of our 10 recommendations. It also described actions planned and under way to implement the 9 recommendations. In particular, the department said that to fully establish a cyber analysis and warning capability, it plans to continue expansion of the Einstein intrusion detection system and increase US-CERT's staffing. In addition, to address the challenges that impede DHS from fully implementing key cyber analysis and warning attributes, the department stated that it plans to continue to build new relationships and grow existing ones with stakeholders. Further, to strengthen its analysis and warning capability and develop its predictive analysis capability, the department cited, among other things, its planned implementation of an upgraded version of Einstein.

DHS took exception to our last recommendation, stating that the department had developed a concept-of-operations document that clearly defined roles and responsibilities for the National Cybersecurity Center and NCSD. However, this concept-of-operations document is still in draft, and the department could not provide a date for when the document would be finalized and implemented.

DHS also commented on the report's description of US-CERT as "the center." Specifically, DHS was concerned that referring to US-CERT as the center might lead to confusion with the department's newly established National Cybersecurity Center. DHS requested that we remove references to US-CERT as the center. We agree with this comment and have incorporated it in the report where appropriate.

In addition to its written response, the department provided technical comments that have been incorporated in the report where appropriate.

We also incorporated technical comments provided by other entities involved in this review.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees, the Secretary of Homeland Security, and other interested parties. We also will make copies available to others upon request. In addition, this report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact David Powner at (202) 512-9286, or pownerd@gao.gov, or Dr. Nabajyoti Barkakati at (202) 512-4499, or barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report are listed in appendix III.

David A. Powner
Director, Information Technology Management Issues

Dr. Nabajyoti Barkakati
Acting Chief Technologist

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) identify key attributes of cyber analysis and warning capabilities, (2) compare these attributes with the United States Computer Emergency Readiness Team's (US-CERT) current analysis and warning capabilities to identify whether there are gaps, and (3) identify US-CERT's challenges to developing and implementing key attributes and a successful national cyber analysis and warning capability.

To identify key attributes of cyber analysis and warning capabilities, we identified entities based on our previous work related to cyber critical infrastructure protection, information security, and information sharing and analyzed relevant laws, strategies, and policies. In addition, we solicited suggestions from a variety of sources familiar with cyber analysis and warning organizations, including GAO's chief information technology officer and members of our Executive Council on Information Management and Technology, which is a group of executives with extensive experience in information technology management who advise us on major information management issues affecting federal agencies. On the basis of the entities identified, we selected those that were relevant and agreed to participate. We then gathered and analyzed policies, reports, and surveys; made site visits to observe the operation of cyber analysis and warning capabilities; conducted structured interviews; and received written responses to structured interview questions. These activities were performed, as appropriate, at the following entities:

- Department of Defense: Commander and Deputy Commander of the Joint Task Force—Global Network Operations and Director of the Defense Information Systems Agency; Commanding Officer, Navy Cyber Defense Operations Command; Chief Information Officer and Electronic Data Service officials of the Navy's Global Network Operations Center. We also toured the Joint Task Force's Global Network Operations Center; the Navy's Cyber Defense Operation Command Center; and the Navy Marine Corps Intranet Network's Operations Center, Computer Incident Response Team Laboratory, Request Management Center, and Enterprise Global Networks Operations Center.

- Department of Energy: the Associate Chief Information Officer for Cyber Security for the Department of Energy and other relevant officials, and the Chief Information Officer of the National Nuclear Security Administration and other relevant officials.

- Department of Homeland Security: the Director of the National Cyber Security Division, the Acting Director of the National Cyber Security Division, and the Acting Director of US-CERT.

- National Institute of Standards and Technology: the Director of the Information Technology Laboratory and officials from the Information Technology Laboratory's Computer Security Division.

- Private sector: Carnegie Mellon University's CERT® Coordination Center, Internet Storm Center, LUMETA, Microsoft, MITRE, National Association of State Chief Information Officers, SANS Institute, SRI International, and Symantec.

- Information sharing and analysis centers representing the following sectors: financial services, information technology, states, surface transportation, and research and education.

- Federal agencies in the intelligence community.

On the basis of the evidence gathered and our observations regarding each entity's capabilities and operations, we determined the key common attributes of cyber analysis and warning capabilities. To verify the attributes we identified, we solicited comments from each entity regarding the attributes identified and incorporated the comments as appropriate.

To determine US-CERT's current national analysis and warning capabilities and compare them with the attributes identified to determine whether there were any gaps, we gathered and analyzed a variety of US-CERT policies, procedures, and program plans to identify the organization's key activities related to cyber analysis and warning. We also observed US-CERT operations. In addition, we held interviews with key US-CERT officials, including the Director and Acting Director of the National Cyber Security Division, the Acting Director and Deputy Director of the US-CERT, and other relevant officials, to further clarify and confirm the key initiatives we identified through our analysis of the aforementioned documents. In addition, we interviewed the Director of Intelligence for the Department of Homeland Security's Homeland Infrastructure Threat and Risk Analysis Center to determine that organization's interaction with US-CERT and its role regarding identifying cyber threats. We also interviewed the Deputy Director of the Department of Homeland Security's National Cybersecurity Center to obtain information about its concept-of-operations document. We then compared those activities to the key attributes of cyber analysis and warning capabilities in order to determine US-CERT's ability to provide cyber analysis and warning and identify any related gaps.

To identify US-CERT's challenges to developing and implementing the key attributes and a successful national cyber analysis and warning capability, we gathered and analyzed relevant documents, such as past GAO reports and studies by various cybersecurity-related entities, and interviewed key federal and nonfederal officials regarding the challenges associated with cyber analysis and warning. On the basis of the information received and our knowledge of the issues, we determined the major challenges to developing and implementing the key attributes and a successful national cyber analysis and warning capability.

We performed this performance audit between June 2007 and July 2008 in the Washington, D.C., metropolitan area; Atlanta, Georgia; Bloomington, Indiana; Pittsburgh, Pennsylvania; and Norfolk, Virginia; 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: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

US GAO

2008 JUL -3 PM 2:52

Homeland Security

July 2, 2008

Mr. David Powner
Director
Information Technology Management Issues
United States Government Accountability Office
441 G Street, N.W.
Washington, DC 20001

Dear Mr. Powner:

Re: Draft Report GAO-08-588, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability* (GAO Job Code 310851)

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the subject draft report. We recognize that cyber threats are growing and are increasing in sophistication and accuracy. We also realize that as technology advances and our dependence on an interconnected cyberspace grows, the risks associated with cyber threats increase. The Department's National Protection and Programs Directorate (NPPD) National Cyber Security Division (NCSD) and its United States Computer Emergency Readiness Team (US-CERT)[1] are significantly changing and growing to address these cyber threats.

The federal government has undertaken a National Cybersecurity Initiative (NCI), which includes programs that strengthen US-CERT's capabilities for analyzing malicious activity, issuing warnings, and responding to incidents. With its newly expanded mission, budget and staff and a more customer-driven and outcome oriented culture, US-CERT will continue to increase its cyber analysis and warning capabilities. As US-CERT moves forward, the organization will work to address various recommendations set forth by GAO.

US-CERT is continually working to establish more effective outcome measures that will inform our program delivery and focus our resources on the most prevalent and highest risk issues. In addition to metrics analysis, US-CERT will continue to work with partners to determine how we can address the deficiencies identified by the GAO.

[1] Note: The Department requests that GAO use the acronym, "US-CERT," when referring to the United States Computer Emergency Readiness Team and remove any references to it as "the center." US-CERT is not classified or defined as a center by the Department or any other entity. The GAO's use of the term "the center" can be confusing because the report also refers to the National Cyber Security *Center* (NCSC), which is an organization separate from NCSD. The NCSC will not duplicate the roles and responsibilities of the participating organizations, such as US-CERT, but will support them and ensure coordination and shared cyber security situational awareness across these organizations.

www.dhs.gov

GAO Recommendation 1: *We recommend that the Secretary of Homeland Security–to fully establish a national cyber analysis and warning capability–specifically address deficiencies in monitoring, including establish a comprehensive baseline understanding of the nation's critical information infrastructure and engage appropriate nonfederal stakeholders to support a national-level cyber monitoring capability.*

Response: US-CERT concurs with this recommendation. Under the NCI, US-CERT is expanding its initial EINSTEIN program, referred to as EINSTEIN 1. The expanded program, referred to as EINSTEIN 2, is a 24x7 intrusion detection system that gathers network flow data from federal agencies and analyzes traffic patterns and behaviors. To improve US-CERT's capability to maintain situational awareness, all federal executive agencies, in accordance with the Office of Management and Budget (OMB) November 20, 2007, Memorandum M-08-05, Implementation of Trusted Internet Connection, will be required to use EINSTEIN 2. This expanded use of EINSTEIN 2 enables the US-CERT to gain increased situational awareness from all the federal executive agencies and fulfill its mandate to act as a central point for computer network security of the federal enterprise.

US-CERT does not directly monitor malicious activity involving nonfederal networks. However, NPPD and US-CERT actively reach out to private sector partners via various mechanisms to develop a baseline understanding of the nation's critical information infrastructure. NPPD Protective Security Advisors (PSAs) within the Office of Infrastructure Protection are located in field offices across the country and regularly conduct site visits to assess vulnerabilities, including cyber vulnerabilities, at Critical Infrastructure/Key Resource (CIKR) facilities. Further, NCSD co-chairs the Cross Sector Cyber Security Working Group under the National Infrastructure Protection Plan (NIPP) Framework, which includes representatives from all CIKR sectors and provides a monthly venue for engagement, collaboration and information sharing on cyber security issues.

A specific example of how the Department identifies specific vulnerabilities in the Nation's critical information infrastructure is the AURORA scenario, which involves the protective control systems used in the Nation's electric power grid. As soon as DHS identified this vulnerability, a Tiger Team of subject matter experts from government and industry was convened to determine the scope, potential consequences of this vulnerability, and to develop a better system for guiding private industry efforts to secure control systems. DHS is currently working with its government and industry partners to closely monitor this vulnerability, asses the risk it poses, and take appropriate proactive measures.

GAO Recommendation 2: *We recommend that the Secretary of Homeland Security–to fully establish a national cyber analysis and warning capability- specifically address deficiencies in analysis, including expanding its capabilities to investigate incidents.*

Response: We concur and are actively implementing improvements that will address the recommendation. Since January 2008, there has been an increase in funding of $115M in Fiscal Year 2008 for US-CERT. This funding includes salaries and benefits for 35 additional federal personnel and related costs, which will allow US-CERT to increase its cyber analysis and warning capabilities.

Much of the increased funding will be focused on developing and deploying EINSTEIN 2. EINSTEIN 2, like EINSTEIN 1, will continue to passively observe network traffic to and from participating federal executive agencies' networks. In addition, EINSTEIN 2 will alert when specific malicious network activity is detected and provide US-CERT with increased insight into the nature of that activity. Through EINSTEIN 2, US-CERT will be able to analyze malicious activity occurring across the federal IT networks resulting in improved computer network security situational awareness. This increase in situational awareness can then be shared with federal executive agencies in an effort to reduce and prevent computer network vulnerabilities.

EINSTEIN 2 adds to EINSTEIN 1 a network intrusion detection technology that will monitor for malicious activity in network traffic to and from participating federal executive agencies. EINSTEIN 2 will alert US-CERT when the system identifies malicious network traffic occurring in a federal executive agencies' network in response to specific predefined signatures. By scanning communications during transmission, EINSTEIN 2 identifies harmful communications that warrant analysis. A US-CERT analyst may then query that specific information in EINSTEIN 2 to analyze the potentially harmful network traffic identified by the alert.

EINSTEIN 2 is to augment -- not replace or reduce -- the current computer network security practices of participating federal executive agencies. Participating agencies will continue to operate their own intrusion detection and prevention systems, perform network monitoring, and use other information security technologies. EINSTEIN 2 enables US-CERT to correlate activity across the entire federal enterprise. With the enhanced correlation capability, US-CERT achieves increased situational awareness of federal executive agency computer networks which is required to perform the computer network security responsibilities assigned to DHS.

GAO Recommendation 3: *We recommend that the Secretary of Homeland Security- to fully establish a national cyber analysis and warning capability- specifically address deficiencies in warning, including ensuring consistent notifications that are targeted, actionable, and timely.*

Response: We concur with the recommendation. A key goal of US-CERT is to ensure that alerts—Critical Infrastructure Information Notices (CIINs) in particular—reach the appropriate stakeholders. US-CERT recognizes the importance of targeted information sharing and is working with NCSD's Outreach and Awareness Program and other cross sector working groups to increase awareness and communication channels.

The following communication channels are currently used for notification and activation in the event of a Cyber Incident:

- The National Cyber Alert System: This system provides an infrastructure, managed by US-CERT, for relaying timely and actionable computer security updates and warning information to all users.
- National Operations Center: This is the primary national-level hub for domestic incident management communications and operations.
- Homeland Security Information Network (HSIN) Critical Sector (CS): This communications network provides States and critical infrastructure owners and operators with real-time interactive connectivity to the National Operations Center (NOC) on a

Sensitive-but-Unclassified (SBU) level to all users. HSIN-CS is the NOC's primary suite of tools for information sharing, coordination, planning, mitigation, and response.

- US-CERT Portal: This secure collaboration tool enables private and public sectors to actively share information about cyber security vulnerabilities, exploits, and incidents in a trusted and secure environment among members.
- US-CERT Public Web Site: www.uscert.gov provides the primary means for US-CERT to convey information to the public at large. The site includes relevant information on cyber security issues, cyber activity, and vulnerability resources.
- Information Sharing and Analysis Centers (ISACs): Through secure websites and secure e-mail, information on infrastructure threats and vulnerabilities is provided to the members.

We do not agree with the report's repeated description of US-CERT's warnings and notifications as "not consistently actionable or timely (*i.e.*, providing the right information to the right person or group when needed)." We believe this statement inaccurately generalizes all US-CERT products. While US-CERT is charged with analyzing cyber threats and disseminating warning information, it relies on other stakeholders and entities such as ISACs, State, local, and tribal entities to review and maintain an accurate list of members who disseminate information to the correct personnel within their organization.[2]

GAO Recommendation 4: *We recommend that the Secretary of Homeland Security–to fully establish a national cyber analysis and warning capability–specifically address deficiencies in response, including ensuring that US-CERT provides assistance in the mitigation and recovery from simultaneous severe incidents, including incidents of national significance.*

Response: We concur and are actively implementing improvements for addressing the recommendation. While the Department is constantly enhancing its capabilities and currently increasing its budget and staffing, we do have recent examples of success in mitigating the effects of cyber incidents.

The GAO report mentioned the May 2007 denial-of-service cyber attack in Estonia; US-CERT successfully mitigated the effects of this attack. Bot-networks were flooding Estonia's IT systems with traffic, causing a denial of service for many of their government sites. US-CERT coordinated with its federal, international, and private sector partners to identify over 2,500 unique sources from 21 NATO countries participating in the attacking botnets on Estonia. The information was shared with military, intelligence, law enforcement, and US-CERT personnel from NATO member nations.

The GAO report also mentioned the Cyber Storm II exercise. The Cyber Storm II exercise, hosted by the Department of Homeland Security, helped participating organizations—public and private—prepare for, respond to, and mitigate cyber attacks that could affect their ability to

[2] With regard to targeted dissemination of US-CERT's vetted products [*e.g.*, Federal Information Notices (FINs), US-CERT CIINs issued via the Homeland Security Information Network – Critical Sectors (HSIN-CS) portal, and Situational Awareness Reports (SARs) US-CERT only vets the membership for the Government Forum of Incident Response and Security Teams (GFIRST)].

deliver critical services. This exercise is one of DHS's primary methods for enhancing crisis management and improving risk management across all participating organizations and highlights the interdependencies that exist between cyber and physical infrastructure. The exercise included elements of the private sector in the transportation, chemical, information technology, and communications sectors as well as federal agencies and departments and several international partners.

Also, EINSTEIN has proven successful in enhancing security within the federal government. Through the Department of Transportation's (DOT's) participation in the EINSTEIN program, US-CERT was able to quickly detect malicious activity and prevent it from infecting other government computers. In this case, a computer worm had infected an unsecured government computer in a U.S. Government agency. When the worm attempted to attack DOT's network, EINSTEIN detected the unusual traffic, and the subsequent US-CERT investigation uncovered the worm and worked with the affected departments and agencies to prevent its spread.

GAO Recommendation 5: *We recommend that the Secretary address the challenges that impede DHS from fully implementing the key attributes, including engaging appropriate stakeholders in federal and nonfederal entities to determine ways to develop closer working and more trusted relationships.*

Response: We concur and are actively implementing approaches for addressing the recommendation. Significant progress has been made in establishing or strengthening relationships with stakeholders, both internationally and domestically. The Department will continue to build new relationships and grow existing ones.

US-CERT coordinates information sharing and incident response activities with international partners to improve cyber incident response at the international level. US-CERT representatives participate in conferences to enhance international cyber coordination. US-CERT also meets individually with other countries' CERTs to discuss cyber incident mitigation and response strategies.

NCSD is committed to providing timely and actionable information on cyber incidents so that State cyber security responders can take appropriate action. Also, the information provided by State/local partners supplies important situational awareness for NCSD. There are channels in place that DHS uses to disseminate cyber information to State and local homeland security stakeholders.

- Government Forum of Incident Response and Security Teams (GFIRST): NCSD recently extended GFIRST membership to State and local governments. This is very significant as it links technical cyber experts in federal agencies with their counterparts in State/local governments and provides State/local governments access to tools and additional technical analysis. The GFIRST forum provides these technical experts with a collaborative space that will increase States' situational awareness of cyber incident response activity. US-CERT products and alerts are sent via the US-CERT-managed GFIRST portal.

- Multi-State Information Sharing and Analysis Center (MS-ISAC): The MS-ISAC membership is comprised of cyber officials from all States. NCSD provides funding to

the MS-ISAC to assist with State/local coordination and information sharing on operational and other cyber security activities. NCSD provides a dedicated secure compartment within the US-CERT portal to enable collaboration among the State/local community and with NCSD/US-CERT. NCSD uses the Portal to both coordinate cyber awareness activities and initiatives, as well as disseminate critical cyber alerts and information. The MS-ISAC also maintains a distribution list of State and local points of contact, which allows NCSD to reach out to State/local decision makers regarding challenges, needs, and opportunities. In addition, NCSD participates in monthly calls with MS-ISAC membership and provides updates on Department activities and works with State/local representatives through established working groups that meet via monthly conference calls.

- Lessons Learned Information Sharing: NCSD has created a cyber security page on the LLIS.GOV site, which all homeland security personnel at the State and local level can access. NCSD populated this page with information regarding exercise after action reports, awareness materials, policies, plans, and other information on cyber security. States can post their best practices and materials here as well.

- Direct Contact: NCSD/US-CERT maintains positive relationships with numerous State points of contact and communicates/collaborates with them directly on a variety of topics.

GAO Recommendation 6: *We recommend that the Secretary address the challenges that impede DHS from fully implementing the key attributes, including expeditiously hiring sufficiently trained cyber analysts and developing strategies for hiring and retaining highly qualified cyber analysts.*

Response: We concur with the recommendation, and a strategy is already in place to address this need. DHS has recently entered into a contract to develop and implement a recruitment strategy to assist with cyber-related vacancies. NPPD has established an agreement with the Office of Personnel Management (OPM) to put a contracted human capital team in place to support the hiring requirement.

Vacancies are posted through a variety of internal and external mechanisms, including less traditional federal government venues, such as recruiting websites and various local newspapers. DHS and US-CERT participate in various career fairs and accepts referrals from other agencies and employees. Graduating students are also targeted through the Scholarship for Service program.

GAO Recommendation 7: *We recommend that the Secretary address the challenges that impede DHS from fully implementing the key attributes, including identifying and acquiring technological tools to strengthen cyber analytical capabilities and handling the steadily increasing workload.*

Response: We concur and are actively implementing approaches that address the recommendation. As described above, US-CERT is implementing an upgraded version of Einstein. Einstein 2 is an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal government so that Federal agencies are aware,

in near real-time, of threats to infrastructure and can act swiftly to take corrective measures. It will incorporate network intrusion detection technology capable of alerting US-CERT to the presence of malicious or potentially harmful computer network activity in Federal executive agencies' network traffic.

In addition to implementing US-CERT's Einstein 2, DHS' Office of Science and Technology (S&T) and CS&C collaborate on cyber research and development (R&D) priorities to identify and develop technological tools to strengthen cyber analytical capabilities. Specifically, S&T created an Integrated Product Team (IPT) process to ensure proponents of R&D requirements, such as CS&C, are able to provide their requirements to S&T (i.e., existing capability shortfalls). A Research, Development, Test and Evaluation (RDT&E) program was established by S&T to address these requirements. CS&C developed a list of cyber security RDT&E requirements for the NCI which are in the process of being forwarded to S&T. These cyber related RDT&E requirements for critical infrastructures have been developed in a government-industry consensus process and are specified in the R&D portions of the Communications and IT Sector Specific Plans.

GAO Recommendation 8: *We recommend that the Secretary address the challenges that impede DHS from fully implementing the key attributes, including developing predictive analysis capabilities by defining terminology, methodologies, and indicators, and engaging appropriate stakeholders in other federal and nonfederal entities.*

Response: We concur and are actively implementing approaches that address the recommendation. EINSTEIN 2 uses anomaly-based detection methods to identify harmful or malicious computer network incidents. Anomaly-based detection, as defined in NIST Special Publication 800-94, is defined as "the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations."

While an intrusion detection system uses a defined set of rules or filters that have been crafted to catch a specific, malicious event, the EINSTEIN 2 anomaly detection capability utilizes the network flow data and alerts to focus on the system's baseline of normal activity. As described above, behavior that varies from this standard is noted. Intrusion detection systems look for a misuse signature and anomaly detection looks for a strange event.

NCSD is also working with other Departmental and Interagency components to develop the strategic analysis of the Nation's critical cyber infrastructure, integrating all relevant and appropriate sources of information to support predictive analysis. NCSD is also seeking to engage stakeholders in other federal and nonfederal agencies to provide them with actionable information based on this predictive analysis.

GAO Recommendation 9: *We recommend that the Secretary address the challenges that impede DHS from fully implementing the key attributes, including filling key management positions and developing strategies for hiring and retaining those officials.*

Response: We concur with this recommendation. However, it is important to note that since the Exit Conference NCSD has filled several key management positions, including the positions of NCSD Director, US-CERT Director of Operations, and NCSD Chief of Staff. Further, DHS has recently entered into a contract to develop and implement a recruitment strategy to assist with

cyber-related vacancies. NPPD has established an agreement with the Office of Personnel Management (OPM) to put a contracted human capital team in place to support the hiring requirement.

GAO Recommendation 10: *We recommend that the Secretary address the challenges that impede DHS from fully implementing the key attributes, including ensuring that there are distinct and transparent lines of authority and responsibility assigned to DHS organizations with cybersecurity roles and responsibilities, including the Office of Cyber Security and Communications and the National Cyber Security Center.*

Response: We do not concur with this recommendation. During the time period that GAO conducted their Cyber Analysis and Warning review, extensive interagency collaboration and coordination took place. This resulted in a NCSC Concept of Operations (CONOPS) with clearly defined roles and responsibilities for NCSC and NCSD. NCSC coordinates cyber security efforts and improves situational awareness and information sharing to support the entities defending government networks, such as US-CERT. US-CERT's ability to synthesize information and provide situational awareness will be enhanced through its work with the NCSC. The NCSC does not duplicate the roles and responsibilities of the participating organizations, such as US-CERT, but supports them in their mission and ensures coordination and shared cyber security situational awareness across these organizations.

Sincerely,

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

David A. Powner, (202) 512-9286 or pownerd@gao.gov
Dr. Nabajyoti Barkakati, (202) 512-4499 or barkakatin@gao.gov

Staff Acknowledgments

In addition to the persons named above, Neil Doherty, Michael Gilmore, Barbarol James, Kenneth A. Johnson, Kush K. Malhotra, Gary Mountjoy, Jennifer Stavros-Turner, and Amos Tevelow 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). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, 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, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548