United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2008

CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise

GAO-08-825

September 2008

CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-825, a report to congressional requesters

Why GAO Did This Study

Federal policies establish the Department of Homeland Security (DHS) as the focal point for the security of cyberspace. As part of its responsibilities, DHS is required to coordinate cyber attack exercises to strengthen public and private incident response capabilities. One major exercise program, called Cyber Storm, is a large-scale simulation of multiple concurrent cyber attacks involving the federal government, states, foreign governments, and private industry. To date, DHS has conducted Cyber Storm exercises in 2006 and 2008.

GAO agreed to (1) identify the lessons that DHS learned from the first Cyber Storm exercise, (2) assess DHS's efforts to address the lessons learned from this exercise, and (3) identify key participants' views of their experiences during the second Cyber Storm exercise. To do so, GAO evaluated documentation of corrective activities and interviewed federal, state, and private sector officials.

What GAO Recommends

GAO is recommending that DHS schedule and complete the corrective activities identified to address lessons learned during the first Cyber Storm exercise, many of which were reiterated during the second Cyber Storm exercise. In written comments, DHS agreed with this recommendation and reported on its efforts to complete corrective activities.

To view the full product, including the scope and methodology, click on GAO-08-825. For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

As a result of its first Cyber Storm exercise, in February 2006, DHS identified eight lessons that had significant impact across sectors, agencies, and exercise participants. These lessons involved improving (1) the interagency coordination groups; (2) contingency planning, risk assessment, and roles and responsibilities; (3) integration of incidents across infrastructures; (4) access to information; (5) coordination of response activities; (6) strategic communications and public relations; (7) processes, tools, and technology; and (8) the exercise program.

While DHS has demonstrated progress in addressing the lessons it learned from its first Cyber Storm exercise, more remains to be done to fully address the lessons. In the months following its first exercise, DHS identified 66 activities that address one or more of the lessons, including hosting meetings with key cyber response officials from foreign, federal, and state governments and private industry, and refining their operating procedures. To date, DHS has completed a majority of these activities (see table). However, key activities have not yet been completed. Specifically, DHS identified 16 activities as ongoing and 7 activities as planned for the future. Further, while DHS has identified completion dates for its planned activities, it has not identified completion dates for its ongoing activities. Until DHS schedules and completes its remaining activities, the agency risks conducting subsequent exercises that repeat the lessons learned during the first exercise.

Commenting on their experiences during the second Cyber Storm exercise, in March 2008, participants observed both progress and continued challenges in building a comprehensive national cyber response capability. Their observations addressed several key areas, including the value and scope of the exercise, roles and responsibilities, public relations, communications, the exercise infrastructure, and the handling of classified information. For example, many participants reported that their organizations found value in the exercise because it led them to update their contact lists and improve their response capabilities. Other participants, however, reported the need for clarifying the role of the law enforcement community during a cyber incident and for improving policies governing the handling of classified information so that key information can be shared. Many of the challenges identified during Cyber Storm II were similar to challenges identified during the first exercise.

Summary of Status of Activities

Status of DHS activities	Number of activities
Reported and validated as completed	42
Reported as completed, but not validated due to insufficient evidence	1
Reported as ongoing	16
Reported as planned for the future	7
Total	**66**

Source: GAO analysis of DHS data.

Contents

Tables

Figure

Abbreviations

DHS	Department of Homeland Security
ISAC	Information Sharing and Analysis Center
NCRCG	National Cyber Response Coordination Group
NCSD	National Cyber Security Division
US-CERT	United States Computer Emergency Readiness Team

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 9, 2008

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

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

Since the early 1990s, 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 of this technology have been enormous, this widespread interconnectivity poses significant risks to the government's and our nation's computer systems and, more important, to the critical operations and infrastructures they support.

Federal policies establish the Department of Homeland Security (DHS) as the focal point for the security of cyberspace—including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for public and private critical infrastructure systems.[1] To accomplish this mission, DHS is to work with federal agencies, state and local governments, and the private sector. Federal policy also recognizes the importance of building public/private partnerships because the private sector owns a large percentage of the nation's critical infrastructure—including banking and financial institutions, telecommunications networks, and energy production and transmission facilities.

As part of DHS's cybersecurity responsibilities, the agency is required to coordinate cyber attack simulation exercises to strengthen public and

[1]The White House, *National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003), and Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (Dec. 17, 2003).

private incident response capabilities. One major exercise program, called Cyber Storm, is a large-scale simulation of multiple concurrent cyber attacks involving the federal government, states, foreign governments, and private industry. To date, DHS has conducted Cyber Storm exercises in 2006 and 2008, and it is currently planning a third for 2010. Because of your interest in these exercises, we agreed to (1) identify the lessons that DHS learned from the first Cyber Storm exercise, (2) assess DHS's efforts to address the lessons learned from this exercise, and (3) identify key participants' views of their experiences during the second Cyber Storm exercise.

To address these objectives, we reviewed relevant DHS documents, including the Cyber Storm I Exercise Report, a list of planned post-Cyber Storm activities, and artifacts showing actions taken to address activities. We attended the second Cyber Storm exercise, held in Washington, D.C., in March 2008. We also interviewed DHS officials responsible for planning the exercises as well as participants in the Cyber Storm exercises, including officials representing three federal agencies, three private industry sectors, and one representing state governments. In addition, this work builds on a body of work we have done over the last several years on the cyber aspects of critical infrastructure protection.[2]

We performed our work from January to September 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

[2]GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005); *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*, GAO-05-827T (Washington, D.C.: July 19, 2005); *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006); *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO-06-863T (Washington, D.C.: July 28, 2006); *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity Elements*, GAO-06-1087T (Washington, D.C.: Sept. 13, 2006); *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007); *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-08-119T (Washington, D.C.: Oct. 17, 2007); *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-113 (Washington, D.C.: Oct. 31, 2007).

audit objectives. Additional details on our objectives, scope, and methodology are provided in appendix I.

Results in Brief

As a result of its first Cyber Storm exercise, in February 2006, DHS identified eight lessons that had significant impact across sectors, agencies, and exercise participants. These lessons involved improving (1) the interagency coordination groups; (2) contingency planning, risk assessment, and roles and responsibilities; (3) integration of incidents across infrastructures; (4) access to information; (5) coordination of response activities; (6) strategic communications and public relations; (7) processes, tools, and technology; and (8) the exercise program.

While DHS has demonstrated progress in addressing the lessons it learned from its first Cyber Storm exercise, more remains to be done to fully address the lessons. In the months following its first exercise, DHS identified 66 activities that address one or more of the lessons, including hosting meetings with key cyber response officials from foreign, federal, and state governments and private industry; refining operating procedures; and obtaining new tools and technologies to support incident response operations. Since that time, DHS has completed 42 of these activities.[3] However, key activities have not yet been completed. DHS identified 16 activities as ongoing and 7 as planned for the future. In addition, while DHS identified completion dates for its planned activities, it has not identified completion dates associated with activities that are reported as ongoing. For example, DHS reports that it has work under way to issue guidance to information sharing and analysis centers on public communications related to cybersecurity, but has not established a milestone for completing this activity. Until DHS schedules and completes its remaining activities, the agency risks conducting subsequent exercises that repeat the lessons learned during the first exercise.

Commenting on their experiences during the second Cyber Storm exercise in March 2008, participants observed both progress and continuing challenges in building a comprehensive national cyber response capability. Their observations addressed several key areas, including the value and scope of the exercise, roles and responsibilities, public relations, communications, the exercise infrastructure, and the handling of classified

[3]DHS reported that one other activity had been completed, but the department was unable to provide evidence demonstrating its completion.

information. For example, many participants reported that their organizations found value in the exercise because it led them to update their contact lists and improve their response capabilities. Other participants, however, reported the need for clarifying the role of the law enforcement community during a cyber incident and for improving policies governing the handling of classified information so that key information can be shared. Many of the challenges noted during Cyber Storm II were similar to ones identified during the first exercise.

We are making a recommendation to the Secretary of Homeland Security to direct the Assistant Secretary for Cybersecurity and Communications to oversee the completion of corrective activities resulting from Cyber Storm I, many of which were reiterated during Cyber Storm II. DHS provided written comments on a draft of this report (see app. IV). In its comments, DHS concurred with our recommendation and reported that the department is working to complete applicable activities identified during the first Cyber Storm exercise. DHS officials also provided technical comments, which we have incorporated as appropriate.

Background

Critical infrastructures are physical or virtual systems and assets so vital to the nation that their incapacitation or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of these matters. These systems and assets—such as the electric power grid, chemical plants, and water treatment facilities—are essential to the operations of the economy and the government. Recent terrorist attacks and threats have underscored the need to protect our nation's critical infrastructures. If vulnerabilities in these infrastructures are exploited, they could be disrupted or disabled, leading to physical damage, economic losses, and even loss of life.

The Federal Government Plays a Critical Role in Helping Secure Critical Infrastructures

Federal law and policies call for critical infrastructure protection activities to enhance the physical and cybersecurity of both public and private infrastructures that are essential to national security, economic well-being, and national public health and safety.[4] Federal policies identify 18 critical infrastructure sectors and designate certain federal agencies as lead points of contact for each (see table 1). Further, they assign these agencies responsibility for infrastructure protection activities in their assigned sectors and for coordination with other relevant federal agencies, state and local governments, and the private sector. In addition, federal policies establish DHS as the focal point for the security of cyberspace—including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for public and private critical infrastructure systems.

Table 1: Critical Infrastructure Sectors and Their Lead Agencies

Sector	Description	Lead agency
Agriculture and food	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production, processing, and retail sales.	Department of Agriculture, Department of Health and Human Services, Food and Drug Administration [a]
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions, including clearing and settlement.	Department of the Treasury
Chemical	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical industry produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.	Department of Homeland Security
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.	Department of Homeland Security
Commercial nuclear reactors, materials, and waste	Includes 104 commercial nuclear reactors; research and test nuclear reactors; nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste.	Department of Homeland Security
Dams	Comprises approximately 80,000 dam facilities, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.	Department of Homeland Security

[4]The law and policies include the Homeland Security Act of 2002 (Pub. L. No. 107-296, Nov. 25, 2002); Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (Dec. 17, 2003); and *The National Strategy to Secure Cyberspace* (February 2003).

Sector	Description	Lead agency
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Drinking water and water treatment systems	Sanitizes the water supply through about 170,000 public water systems. These systems depend on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.	Environmental Protection Agency
Emergency services	Saves lives and property from accidents and disasters. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	Department of Homeland Security
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. This sector is divided into electricity and oil and natural gas.	Department of Energy
Government facilities	Includes the buildings owned and leased by the federal government for use by federal entities.	Department of Homeland Security
Information technology	Produces hardware, software, and services that enable other sectors to function.	Department of Homeland Security
National monuments and icons	Includes key assets that are symbolically identified with traditional American values and institutions or U.S. political and economic power.	Department of the Interior
Manufacturing	Includes key critical manufacturing operations based on highly integrated and interdependent supply chains. This sector provides metal, machinery, electrical equipment, appliances, components, and transportation equipment.	Department of Homeland Security
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The United States Postal Service and other carriers provide the services of this sector.	Department of Homeland Security
Public health and health care	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. This sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Telecommunications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.	Department of Homeland Security
Transportation systems	Enables movement of people and assets that are vital to our economy, mobility, and security, using aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	Department of Homeland Security

Source: GAO analysis of The National Infrastructure Protection Plan, Homeland Security Presidential Directive 7, and the National Strategy for Homeland Security.

[a]The Department of Agriculture is responsible for food (meat, poultry, and eggs) and agriculture; and the Department of Health and Human Services, Food and Drug Administration, is responsible for food other than meat, poultry, and egg products.

DHS Organization Is the Focal Point for National Cybersecurity Efforts

In June 2003, DHS created the National Cyber Security Division (NCSD), to serve as a national focal point for addressing cybersecurity issues and to coordinate the implementation of the National Strategy to Secure Cyberspace (the Cyberspace Strategy). Its mission is to secure cyberspace and America's cyber assets in cooperation with public, private, and international entities. NCSD reports to the Assistant Secretary for Cybersecurity and Communications.

A key component of NCSD, the U.S. Computer Emergency Readiness Team (US-CERT), is an operational organization responsible for analyzing and addressing cyber threats and vulnerabilities and disseminating cyber threat warning information. In the event of an Internet disruption, US-CERT facilitates coordination of recovery activities with the network and security operations centers of owners and operators of the Internet and with government incident response teams. We recently reported on US-CERT's challenges in establishing a comprehensive national cyber analysis and warning capability.[5]

NCSD also cochairs the National Cyber Response Coordination Group (NCRCG), which includes officials from the agencies that have a responsibility for cybersecurity as well as the lead agencies for different critical infrastructure sectors.[6] This group is the principal federal interagency mechanism for coordinating the response to and recovery from significant national cyber incidents. In the event of a major incident, NCRCG is responsible for providing subject matter expertise, recommendations, and strategic policy support to the Secretary of Homeland Security.

In addition, DHS recently announced that it is establishing a new National Cyber Security Center that is to report directly to the Secretary of Homeland Security. According to the Assistant Secretary for Cybersecurity and Communications, this center will be responsible for ensuring coordination among the cyber-related efforts across the federal government and improving situational awareness and information sharing to support the entities defending government networks, including US-CERT.

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

[6]The Department of Justice's Computer Crime and Intellectual Property Section and the Department of Defense also cochair this group.

DHS Is Responsible for Conducting and Coordinating Cyber Exercises to Improve National Preparedness, Response, and Recovery Capabilities

Federal policies call for DHS to establish a national exercise program to improve the nation's ability to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies.[7] More specifically, the Cyberspace Strategy calls for DHS to conduct cybersecurity exercises to evaluate the impact of cyber attacks on governmentwide processes and to explore the use of such exercises to test coordination of public and private incident management, response, and recovery capabilities. Further, in its National Infrastructure Protection Plan, DHS states that it will conduct national cyber exercises to improve cyber preparedness, response, coordination, and recovery capabilities. [8]

To address its cyber exercise responsibilities, DHS works with other federal agencies, state and city governments, regional coalitions, and international partners. DHS's role can range from providing cyber scenarios or expertise to local or regional exercises, cosponsoring exercises, or conducting its own large-scale cyber attack simulations (called Cyber Storm exercises). See table 2 for examples of recent and planned cyber exercises.

Table 2: Recent and Planned Cyber Exercises

Date	Exercise name	Description	Participant(s)
September 2004	Blue Cascades II	Cosponsored by DHS and organized by members of the Pacific Northwest Economic Region. This exercise tested regional capabilities to deal with threats, interdependencies, and cascading impacts by simulating a series of attacks that disrupted infrastructures and organizations, including critical telecommunications and electricity assets.	Federal, state, and local governments and private industry
October 2004	Purple Crescent II	Sponsored by the Gulf Coast Regional Partnership for Infrastructure Security and funded by DHS. The exercise was designed to raise awareness of infrastructure interdependencies and identify how to improve regional preparedness by simulating cyber attacks on regional infrastructures as well as government and private organizations during an approaching hurricane.	Federal, state, and local governments; academic institutions; and private industry
April 2005	Top Officials-3	Sponsored by DHS, this exercise was to evaluate decision making by federal, state, and local governments by simulating terrorist threats and attacks involving chemicals, biological agents, and explosives.	Federal, state, local, and foreign governments and private industry

[7]Homeland Security Presidential Directive 8: National Preparedness (Dec. 17, 2003) and *The National Strategy to Secure Cyberspace* (February 2003).

[8]Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006).

Date	Exercise name	Description	Participant(s)
April 2005	Multi-State Information Sharing and Analysis Center's Tabletop Exercise	Cosponsored by DHS and the Multi-State Information Sharing and Analysis Center during the center's annual meeting. This tabletop exercise was designed to offer an opportunity for the state information technology participants to discuss their state policies and procedures and to prepare for the Cyber Storm I exercise.	State governments
February 2006	Cyber Storm I	Sponsored by DHS, Cyber Storm I was the first large-scale national cyber exercise to improve incident response and coordination capabilities by simulating multiple cyber incidents affecting the energy, information technology, telecommunications, and transportation critical infrastructure sectors.	Federal, state, and foreign governments and private industry
March 2006	Blue Cascades III	Cosponsored by DHS and organized by members of the Pacific Northwest Economic Region. This exercise was designed to focus on efforts to recover and restore services by simulating the impact of a major earthquake in the area.	Federal, state, local, and foreign governments and private industry
October 2006	Delaware Cyber Security Tabletop Exercise	Sponsored by the state of Delaware, with assistance from DHS. This exercise was designed to discuss the technical implications of a pandemic disaster scenario.	State government
December 2006	Cyber Tempest	Cosponsored by DHS and the New York State Office of Cyber Security and Critical Infrastructure Coordination. This exercise was designed to focus on regional stakeholders' procedures for response and coordination during emergencies.	State governments
April 2007	Multi-State Information Sharing and Analysis Center's Tabletop Exercise	Cosponsored by DHS and the Multi-State Information Sharing and Analysis Center during the center's annual meeting. This exercise was designed to offer an opportunity for the state information technology participants to discuss their state policies and procedures and to prepare for the Cyber Storm II exercise.	State governments
September 2007	ChicagoFIRST Exercise	Cosponsored by DHS and ChicagoFIRST, a nonprofit organization representing financial institutions. This exercise was designed to offer the city government an opportunity to collaborate with greater Chicago regional stakeholders.	Local/regional government
October 2007	Top Officials-4	Sponsored by DHS. This exercise was designed to test federal, state, territorial, and local response capabilities by simulating coordinated attacks using a radiological dispersal device.	Federal, state, local, and foreign governments and private industry
October 2007	Illinois Cyber Tabletop Exercise	Sponsored by the state of Illinois, with assistance from DHS. This exercise was designed to provide participants with an opportunity to discuss a cyber scenario affecting multiple state critical infrastructures, resulting in cascading effects across the state.	State government
October 2007	Delaware Cyber Security Tabletop Exercise	Sponsored by the state of Delaware, with assistance from DHS. The exercise was designed to discuss the increasing threat of financial and identify thefts with stakeholders.	State government
March 2008	Cyber Storm II	Sponsored by DHS, this exercise was to improve national incident response and coordination capabilities by simulating physical and cyber attacks against the transportation, information technology, and chemical critical infrastructure sectors.	Federal, state, and foreign governments and private industry

Date	Exercise name	Description	Participant(s)
May 2008	Massachusetts Cyber Exercise	Cosponsored by DHS and the state of Massachusetts. This exercise was to examine processes, procedures, and the operational architecture of system operators, law enforcement officials, local/state government, and several private sector partners in response to specific cyber attack scenarios.	State and local governments
September 2008	ChicagoFIRST Exercise	Cosponsored by DHS and ChicagoFIRST. This exercise is planned to focus on the financial sector.	Private industry

Source: GAO analysis of DHS data.

DHS's Cyber Storm Exercises

DHS's Cyber Storm exercises are intended to examine national preparedness, response, coordination, and recovery efforts when faced with a large-scale cyber incident. Participants include federal and state agencies, private industry representatives, and selected foreign governments. DHS conducted Cyber Storm exercises in 2006 and 2008, and is planning to conduct a third exercise in 2010.

In February 2006, DHS conducted Cyber Storm I at a cost of about $3.7 million. The exercise simulated a large-scale attack affecting the energy and transportation infrastructures, using the telecommunications infrastructure as a medium for the attack. Participants included eight federal departments and three agencies, three states, and four foreign countries. The exercise also involved representatives from the private sector—including 11 information technology companies, 7 electric companies, 1 banking and finance company, and 2 airlines—and over 100 public and private agencies, associations, and corporations. DHS officials conducted the exercise primarily on a separate network to minimize the impact on "real world" information systems. The objectives of Cyber Storm I were to

- exercise interagency coordination by convening NCRCG and the Interagency Incident Management Group, a multi-agency team of federal executives responsible for providing strategic advice during nationally significant incidents;[9]
- exercise intergovernmental and intragovernmental coordination and incident response;
- identify policies and issues that hinder or support cybersecurity requirements;

[9]The Interagency Incident Management Group was later reorganized and renamed the Crisis Action Team.

- identify public/private interface communications and thresholds of coordination to improve cyber incident response and recovery, as well as identify critical information sharing paths and mechanisms;

- identify, improve, and promote public and private sector interaction in processes and procedures for communicating appropriate information to key stakeholders and the public;

- identify cyber and physical infrastructure interdependencies with real world economic and political impact;

- raise awareness of the economic and national security impacts associated with a significant cyber incident; and

- highlight available tools and technologies with analytical cyber incident response and recovery capabilities.

In March 2008, DHS conducted its second broad-scale exercise, called Cyber Storm II. The exercise cost about $6.4 million, and simulated a large-scale cyber attack affecting the communications, information technology, chemical, and transportation infrastructures. According to DHS, the exercise involved 18 federal agencies, 9 states, 10 information sharing and analysis centers, 5 foreign countries, and over 40 industry representatives from the private sector. The objectives of Cyber Storm II were to

- examine the capabilities of participating organizations to prepare for, protect from, and respond to the effects of cyber attacks;

- exercise senior leadership decision making and interagency coordination of incident responses in accordance with national-level policies and procedures;

- validate information sharing relationships and communication paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information; and

- examine the means and processes to share sensitive and classified information across standard boundaries in safe and secure ways without compromising proprietary or national security interests.

DHS plans to issue a report on what it learned from Cyber Storm II by the end of 2008.

DHS Identified Eight Lessons during Cyber Storm I

While Cyber Storm I participants reported that the exercise was valuable in that it helped them establish and improve interagency and public/private response relationships, DHS also identified eight lessons during the Cyber Storm I exercise that affected all participating sectors and agencies. These lessons involved improving (1) the interagency coordination groups; (2) contingency planning, risk assessment, and roles and responsibilities; (3) integration of incidents across infrastructures; (4) access to information; (5) coordination of response activities; (6) strategic communications and public relations; (7) processes, tools, and technology; and (8) the exercise program.

Interagency Coordination Groups

DHS reported that during the exercise, the two key interagency coordination groups—NCRCG and the Interagency Incident Management Group—were convened appropriately and that they worked well together. For example, the two groups coordinated to develop a refined awareness of the attack situation and to assess effects on the nation's critical infrastructure. However, the agency found that a broader understanding of how these groups operate would improve coordination, both within the government and with the private sector. Specifically, participants reported that

- greater collaboration could be achieved if the private sector was allowed interaction with NCRCG during major incidents,
- additional work was needed to determine how to effectively elevate the alert levels in response to cyber attacks or threats,
- NCRCG did not have enough technical experts on staff to fully leverage the large volume of incident information,
- communication procedures were needed to deliver key technical messages at a layman's level to organizations' public affairs groups in a timely manner, and
- an established information sharing process between NCRCG and allied nations would facilitate communication and help ensure a more effective response.

Contingency Planning, Risk Assessment, and Roles and Responsibilities

DHS found that formal contingency planning, risk assessment, and the definition of roles and responsibilities across the entire cyber community must continue to be solidified. It reported that in cases where procedures

were clear and fully understood by participants, incident responses were timely and well coordinated. However, in cases where there were no previously established relationships and procedures for coordinating responses and assessing risks were not clear, participants had difficulty determining which organizations and people to contact. In addition, DHS found that contingency planning for backup or resilient communications was critical. The agency noted that during the exercise many participants relied heavily on communications systems that could be vulnerable to attack or failure.

Integration of Incidents across Infrastructures

According to DHS, the integration of multiple incidents across multiple infrastructures and between the public and private sectors remained a challenge. DHS reported that the cyber incident response community was generally effective in addressing single threats or attacks and, to some extent, in addressing multiple threats and attacks when these incidents were treated as individual and discrete events. However, participants were challenged when attempting to develop an integrated situational awareness and to understand the impact of multiple attacks across sectors. As the organization responsible for analyzing cyber threats and disseminating warnings, US-CERT had a lead role in forming an integrated situational awareness. However, during the exercise, US-CERT was inundated with information and questions from both the public and the private sectors. The US-CERT team found that the volume of information limited its ability to simultaneously provide situational awareness coordination and conduct technical analyses. Participants reported that a prioritization scheme is needed in order to rapidly assess cyber incidents, their sources, and their applicability to the broad-scale attack. In addition, DHS noted that there needs to be greater clarification of US-CERT's roles, responsibilities, and procedures.

Access to Information

While DHS reported that a continuous flow of information created a common framework for responding to the incidents, the majority of exercise participants reported difficulty in identifying accurate and up-to-date sources of information. For example, during the exercise, participants received multiple alerts on a single issue, which created confusion and made it more difficult to establish a single coordinated response. Participants observed that establishing a single point of contact for information would allow a common framework for responses, and noted that US-CERT is the correct agency to disseminate time sensitive and critical information to the appropriate organizations. In addition, while US-CERT provided significant information in the form of alerts and

	technical bulletins, participants stated that US-CERT's capabilities to post information in a timely, secure, and accurate manner needed to be further explored.
Coordination of Response Activities	DHS found that coordinating responses became more challenging as the number of cyber events increased, thus highlighting the importance of cooperation and communication. For example, during the exercise, participants noted the overwhelming effects that multiple, simultaneous, and coordinated attacks had on their response activities, which proved that the ability to accurately fuse information is crucial for responding appropriately to simultaneous attacks. Participants reported that clarifying roles and responsibilities across government, as well as the expectations between public and private sectors, is needed to coordinate preventive measures and responses to disruptions.
Strategic Communications and Public Relations	DHS reported that public messaging must be an integral part of plans for responding to a cyber incident in order to provide critical information to the response community and to empower the public to take appropriate actions. Exercise participants stated that publicly released information could undermine consumer confidence, and noted the importance of aligning both public and private sector public relations plans in order to have a coordinated approach during a crisis. In addition, DHS found that federal responses to cyber incidents must include public affairs teams to ensure that press releases and accurate situation updates are provided to partner organizations and media outlets.
Processes, Tools, and Technology	DHS reported that improved processes, tools, and training for analyzing and prioritizing the physical, economic, and national security impacts of cyber attack scenarios would enhance the quality, speed, and coordination of response. In particular, participants reported that exchanging and sharing classified information was a challenge and suggested that processes be developed to downgrade classified information so that it could be shared throughout the response community.
The Exercise Program	DHS reported that recurring exercises would strengthen participants' awareness of organizational cyber incident response, roles, policies, and procedures. Participants observed that ongoing training, discussions, and exercises are needed to build relationships among organizations and to strengthen the coordination of responses to cyber incidents. In addition,

several participants in Cyber Storm I recommended the execution of smaller, more routine exercises.

DHS Has Demonstrated Progress in Addressing Lessons from Its First Cyber Storm Exercise, but More Remains to Be Done

While DHS has demonstrated progress in addressing the lessons it learned from its first Cyber Storm exercise, more remains to be done to fully address the lessons. Federal policy requires that DHS develop and maintain a system to collect, analyze, and disseminate lessons learned, best practices, and information from exercises, training events, and other sources.[10] In addition, DHS's homeland security exercise program guidance requires that, following an exercise, planners must identify a list of corrective actions and track their implementation.[11]

DHS has begun to fulfill these requirements. Specifically, DHS documented the lessons it learned during the first Cyber Storm exercise and identified 66 activities that address one or more of the lessons. These activities included hosting meetings with key cyber response officials from foreign, federal, and state governments and private industry; refining the procedures under which these entities operate; and participating in smaller cyber exercises to test these refined procedures (see app. II for a list of activities).

In addition, DHS has made progress in completing its planned activities, but more remains to be done. Of the 66 activities intended to address the lessons, 42 activities have been completed. These completed activities range from clarified procedures to improved technology for emergency responders, and they should improve communications and response activities during a significant cyber incident. DHS reported that another activity had been completed, but was unable to provide evidence demonstrating its completion. However, key activities needed to improve coordination and response during a significant cyber incident have not yet been completed. The remaining 23 activities include 16 activities that are ongoing and 7 activities that are planned for the future. While DHS has identified completion dates for its planned activities, it has not identified completion dates associated with activities that are reported as ongoing. For example, DHS reported that it has work under way to issue guidance to information sharing and analysis centers on public communications

[10]Homeland Security Presidential Directive 8: National Preparedness (Dec. 17, 2003).

[11]Department of Homeland Security, *Homeland Security Exercise and Evaluation Program* (Washington, D.C.: 2007).

related to cybersecurity, but has not identified a milestone for completing this activity. Table 3 provides the number of activities in each of these categories.

Table 3: Summary of Status of Activities

Status of DHS activities	Number of activities
Reported and validated as completed	42
Reported as completed, but not validated due to insufficient evidence	1
Reported as ongoing	16
Reported as planned for the future	7
Total	**66**

Source: GAO analysis of DHS data.

Focusing on each of the eight lessons, DHS has completed selected activities within each lesson, but has more to do. The department's progress on each of the lessons learned during the first Cyber Storm exercise is discussed below. In reviewing this progress, it is important to note that because many of DHS's activities are intended to address more than one lesson, the sum of the activities supporting all eight lessons is higher than the net number of activities. Specifically, DHS listed 121 activities to address lessons 1 through 8, but 55 of these repeat a prior activity. A complete list of the activities supporting each lesson and their status are provided in appendix III.

- **Interagency coordination groups**—DHS identified 32 activities to address the need for improving the interagency coordination groups. Of these, 24 activities have been completed and 8 are ongoing or planned for the future. DHS completed activities such as researching and procuring situation awareness visualization and communication tools and conducting a tabletop exercise among NCRCG, the Homeland Security Operations Center, the Crisis Action Team, and US-CERT. Activities that still remain to be completed include establishing secure communications with all international partners and working with leadership to frame possible changes in rules for raising alert levels.

- **Contingency planning, risk assessment, and roles and responsibilities**—DHS identified 15 activities to address the need for improved contingency planning, risk assessment, and roles and responsibilities. Of these, 8 activities had been completed and 7 are ongoing or planned for the future. DHS completed activities such as

researching secure cell phone capability for NCRCG members and procuring satellite phones. Activities that still remain to be completed include coordinating standard operating procedures and concepts of operations with several information sharing and analysis centers and establishing a continuity-of-operations plan.

- **Integration of incidents across infrastructures**—DHS identified 16 activities to address the need for improved integration of incidents across infrastructures. Of these, 9 have been completed and 7 are ongoing or planned for the future. Completed activities include meeting with international participants to share capabilities and establish working relationships and researching alternatives to the Emergency Notification System. Activities that still remain to be completed include filling open spots at US-CERT to better address its mission and coordinating standard operating procedures with US-CERT and the information technology and communications information sharing and analysis centers.

- **Access to information**—DHS identified 15 activities to address the need for improved access to information. Of these, 8 activities have been completed and 7 are ongoing or planned for the future. DHS completed developing a contact list of key public and private sector subject matter experts and meeting with international participants to share capabilities and establish working relationships. Activities that still remain to be completed include identifying and organizing a private sector counterpart for NCRCG and establishing processes, procedures, and physical means to communicate securely with counterparts.

- **Coordination of response activities**—DHS identified 15 activities to address the need for improved coordination of response activities. Of these, 11 have been completed and 4 are ongoing or planned for the future. DHS completed activities such as significantly revising the NCRCG's standard operating procedures and refining situation report development and communication within those procedures. Activities that still remain to be completed include developing policies for handling classified information and educating the law enforcement community on the role and function of NCRCG.

- **Strategic communications and public relations plan**—DHS identified 5 activities to address the lesson that public messaging must be an integral part of contingency planning and incident response. Of these, 1 activity has been completed and 4 are ongoing or planned for the future. DHS completed efforts to establish a mechanism for communicating real world implications of cyber incidents to DHS Public Affairs and the Public Affairs Working Group. Activities that still remain to be completed include

issuing guidance to information sharing and analysis centers on a set of policies for cybersecurity-related public communications and developing public affairs messaging coordination between public and private information technology organizations for normal and emergency operations.

- **Processes, tools, and technology**—DHS identified 12 activities to address the need for improved processes, tools, and technology. Of these, 8 activities have been completed and 4 are ongoing or planned for the future. Completed activities include developing a comprehensive set of cyber scenarios to support the exercises and clarifying interfaces and expectations at every level of NCRCG engagement. Activities that still remain to be completed include requesting that all federal computer emergency response teams obtain secure communications and developing policies for handling classified information.

- **Exercise program**—DHS identified 11 activities to address the need for improvements to the exercise program. Of these, 9 activities have been completed and 2 are ongoing or planned for the future. Completed activities include participating in a tabletop exercise and a full-scale exercise, and improving the communications infrastructure for the exercise. DHS has not yet completed activities including implementing a relational database consistent with industry standards in order to allow better correlation, analysis, and communication of incidents.

  Until DHS schedules and completes its planned corrective activities, the agency risks wasting resources on subsequent exercises that repeat the lessons it learned in its first exercise.

Cyber Storm II Participants Observed Progress and Continued Challenges in Exercising the National Cyber Response Capability

Commenting on their experiences during Cyber Storm II, participants observed both progress and continued challenges in building a comprehensive national cyber response capability. Their observations addressed several key areas, including the value and scope of the exercise, roles and responsibilities, public relations, communications, the exercise infrastructure, and the handling of classified information.

Exercise value and scope—The participants we met with reported that their organization found value in participating in the exercise. For example, one agency official stated that the exercises were invaluable because they allowed the agency to update call lists and to practice how it would respond to cyber events. In addition, a participant stated that the exercise had a positive outcome for his organization and that the real benefit of the exercise was in sharing information.

However, participants agreed that smaller, more frequent exercises would be helpful in planning for cyber incidents. One agency official stated that the "doomsday" scenarios made it difficult to test agencies' responses to less dramatic cyber incidents. Another agency official reported that the sheer number of e-mail alerts received during the exercise was difficult to handle. Another participant suggested that DHS conduct exercises focusing on different infrastructure sectors during every quarterly meeting of NCRCG.

Roles and responsibilities—Cyber Storm II participants reported having a much better understanding of the various organizations' roles and whom to contact within those organizations during a cyber incident. For example, a participant noted that NCRCG has had time to stabilize over the 2 years since the first Cyber Storm exercise.

However, participants also reported that there is room for improvement in defining the roles and responsibilities of both NCRCG and the law enforcement community. Specifically, selected Information Sharing and Analysis Center (ISAC) members reported that there is still confusion in the private sector on NCRCG's role during a cyber incident. ISAC officials stated that it was unclear to the private sector what NCRCG is responsible for, what it means when the group is activated, and what this activation means to the private sector. In addition, Cyber Storm II participants reported the need for further clarification of the roles and responsibilities of the law enforcement community during a cyber incident. Specifically, law enforcement participants noted that other exercise participants may not have been properly reporting incidents to the law enforcement community, even though most scenarios involved criminal violations. They stated that not being appropriately involved in the exercise scenarios made it difficult to fully test investigative and legal processes.

Public relations—While participants generally agreed that media relations went well during the exercise, they also identified the need for further improvements. To address prior concerns, DHS included a public relations specialist in the NCRCG membership to help develop messages for NCRCG and other organizations involved in the exercise, and provided a technical specialist to the department's public affairs office to ensure cyber issues were described accurately. However, a private sector participant commented that there appeared to be minimal alignment of communications and public relations plans between the public and private sectors during the exercise.

Communications—Participants also reported a need for further improvement in communication between participants during the exercise. For example, a private sector participant cited a breakdown in communication where participants were not aware that the US-CERT alert level had been raised. Another participant reported that US-CERT did not resolve conflicting data before issuing information—even after this individual's ISAC contacted US-CERT. In another instance, a private sector participant reported not knowing how to contact US-CERT during the exercise. Another participant reported that there were instances where private sector players were sharing information with DHS, but the information appeared never to have made it to the decision makers.

Exercise infrastructure—Participants generally agreed that improvements to the exercise's infrastructure could be made. For example, several participants reported that DHS was not able to use an encrypted communications system it developed for the exercise because the technology failed. However, DHS reported that the technology did not fail, but rather that it turned off the technology because of security concerns. Participants also reported issues with receiving e-mails of the exercises, downloading the exercise directory, and accessing the exercise's Web page. Another participant stated that his organization did not have time to run some of the exercise scenarios due to technical issues it encountered during the exercise.

Classified information handling—Participants stated that there is a continuing challenge in accessing sensitive information on cyber threats and incidents, and that policies dealing with classified information need to be improved. For example, one private sector participant stated that it is not clear how information gets classified or what information is available to the private sector. An agency official stated that it has been a challenge to pull unclassified information out of classified information systems in order to share it. Other participants stated that they would like to see additional effort expended on sharing unclassified information on the government's public response portal—the Government Forum of Incident Response and Security Teams portal—which is available to federal agencies and to a limited number of local agencies and organizations. Participants noted that the portal is too open for truly secure communication but not open enough to share information between public and private sectors.

Many of the challenges that participants noted during Cyber Storm II were similar to challenges identified during the first Cyber Storm exercise. For example, comments regarding the need for better understanding of roles

and responsibilities after Cyber Storm II were similar to comments made in four of the eight lessons resulting from Cyber Storm I. Also, both exercises resulted in comments calling for improvements to the exercise program and for better internal and external communications.

Conclusions

Both public and private sector participants in DHS's Cyber Storm exercises agreed that the exercises are valuable in helping them coordinate their responses to significant cyber incidents. After the completion of the first Cyber Storm exercise in February 2006, DHS identified 8 lessons and 66 activities to address these lessons, ranging from revising operating procedures to holding tabletop exercises to test and evaluate those revised procedures. While DHS has made progress in completing over 60 percent of these activities, it has more to do to complete key activities—including those that are planned for the future as well as those identified as ongoing without a completion date. More recently, key federal, state, and private sector officials who participated in the second Cyber Storm exercise in March 2008 observed areas of progress as well as continued challenges—many similar to challenges identified during the first exercise. Until DHS schedules and completes its corrective activities, the agency risks wasting resources on subsequent exercises that repeat the lessons it learned in 2006.

Recommendation for Executive Action

Given the importance of continuously improving cyber exercises, we are making one recommendation to the Secretary of Homeland Security to direct the Assistant Secretary for Cybersecurity and Communications to ensure the scheduling and completion of the corrective actions addressing lessons learned during Cyber Storm I before conducting the next Cyber Storm Exercise.

Agency Comments and Our Evaluation

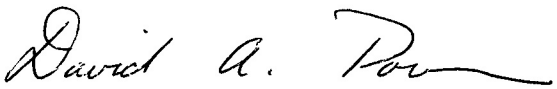
We received written comments on a draft of this report from DHS (see app. IV). In the department's response, the Director of the Departmental GAO/Office of Inspector General Liaison Office concurred with our recommendation and stated that DHS will continue to address actions related to Cyber Storm I findings. DHS also reported that after receiving the draft report, it has completed additional items, raising the percentage of corrective actions completed to over 70 percent. We did not modify the status of the activities identified in our report because DHS has not yet provided sufficient evidence to demonstrate that these activities have been completed.

In its comments, DHS also stated that end dates are not applicable for many of the remaining corrective actions because they are either dependent upon outside stakeholder actions or are ongoing or long-term activities that are being addressed incrementally over time. However, we found that most of the remaining activities are finite in nature and could be associated with a time frame. For example, it would be possible to establish time frames for issuing guidance to the information sharing and analysis centers on public communications, requesting that all computer emergency response teams have secure communications, and identifying international counterparts to NCRCG. Further, while we agree that some activities may involve other stakeholders or take more time, it is important for DHS to identify interim and final milestones for these activities so that they can monitor their progress. This approach is consistent with DHS's guidance for its exercise programs, which requires that each corrective action have a time frame for implementation.

DHS officials also provided technical comments, which we have incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of the 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, the Director of the Office of Management and Budget, and other interested parties. In addition, this report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you have any questions on matters discussed in this report, please contact me at (202) 512-9286 or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.



David A. Powner
Director, Information Technology
Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) identify the lessons that the Department of Homeland Security (DHS) learned from the first Cyber Storm exercise, (2) assess DHS's efforts to implement lessons learned from this exercise, and (3) identify key participants' views of their experiences during the second Cyber Storm exercise.

To identify the lessons learned from DHS's cyber attack simulations, we reviewed the agency's Cyber Storm Exercise Report. We also interviewed agency officials to obtain clarification on this exercise and the lessons learned.

To assess DHS's efforts to address the lessons it learned from its exercise, we analyzed DHS's list of planned activities and the status of these activities. We analyzed documentation of the activities that were reported as completed, including concepts of operations and standard operating procedures for relevant organizations as well as evidence of additional staff hires and completion of tabletop exercises. We also visited the United States Computer Emergency Readiness Team (US-CERT) to observe network and technology changes that were made to address lessons identified during Cyber Storm I. We interviewed DHS officials from the National Cyber Security Division (NCSD) and US-CERT to obtain clarification on documentation and plans.

To identify key participants' views of their experiences during the second Cyber Storm exercise, we interviewed Cyber Storm planners, observers, and participants from federal agencies, state governments, and the private sector. Specifically, we interviewed representatives from the Departments of Transportation, Justice, and Energy because these organizations were identified by DHS as key participants in the Cyber Storm exercises—either as an organization that was subject to simulated cyber incidents or as an organization critical to the recovery from the incidents. We interviewed the Multi-State Information Sharing and Analysis Center (ISAC) because it was able to represent multiple state governments that participated in the exercises. We also interviewed private sector officials representing the Information Technology ISAC, the Electricity ISAC, and the chemical sector. We asked participants about the issues raised during Cyber Storm I and whether these were improved or remained as challenges during Cyber Storm II. After discussing both Cyber Storm exercises with these participants, we analyzed their observations for commonalities and organized them into broad categories. These observations are not intended to be generalized to other exercise participants.

We performed our work at the headquarters of the Departments of Homeland Security, Transportation, Energy, and Justice and in Washington, D.C. In addition, we attended the Cyber Storm II exercise held in Washington, D.C., in March 2008. We performed our work from January 2008 to September 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.

Appendix II: DHS Activities to Address Lessons from Cyber Storm I

DHS identified 66 activities to address lessons identified in Cyber Storm I. Almost half of these activities are intended to address multiple lessons. Table 4 shows the list of activities and which lessons they are intended to address.

Table 4: DHS's Planned Activities and the Lessons They Address

Activity identification number	DHS activity	Lesson(s) targeted by this activity[a]
1.	Significantly revise standard operating procedures for the National Cyber Response Coordination Group (NCRCG)	1, 2, 3, 4, 5, 7, 8
2.	Refine definition of Cyber Incident of National Significance	1
3.	Conduct meeting with member agencies to ensure they understand the needed resources to support NCRCG during activation	1
4.	Establish in standard operating procedures a means of quickly and clearly communicating changes in NCRCG engagement status with interfacing organizations	1, 4
5.	Within standard operating procedures, refine situation reports and situation report development and communication procedures	1, 4, 5, 7, 8
6.	Research and procure appropriate situation awareness visualization and communication tools	1
7.	Request access to classified DHS networks in NCRCG's room	1, 4, 5, 7, 8
8.	Hold meeting among NCRCG, Homeland Security Operations Center, Interagency Advisory Council (now the Crisis Action Team), and US-CERT	1
9.	Conduct a tabletop exercise among NCRCG, the Homeland Security Operations Center, the Interagency Advisory Council (now the Crisis Action Team), and US-CERT	1
10.	Work with the Office of Public Affairs to ensure NCRCG receives situation reports	1
11.	Provide a liaison to an interfacing group from NCRCG	1
12.	During the meeting in June 2006 with international participants, discuss coordination with entities similar to NCRCG	1
13.	Clarify interfaces and expectation at every level of NCRCG engagement	1, 7
14.	Move triage capability into US-CERT main facility	1, 3, 5
15.	Create four new positions to ensure staffing and continuity in US-CERT through normal and emergency operations	1, 7
16.	Refine and prioritize use and purposes of key US-CERT communications portals to eliminate redundancy and streamline communication with subscribers and counterparts	1, 4
17.	Meet in June 2006 with all international participants to share capabilities and establish working relationships	1, 2, 3, 4
18.	Discuss an initial international participant tabletop exercise and additional follow-on exercise activities with international participants and policy representatives in order to build clear way ahead for Cyber Storm II in 2008	1, 3
19.	Coordinate support of DHS's Operations office as noted in its revised standard operation procedures	1, 3, 4, 5, 7

Activity identification number	DHS activity	Lesson(s) targeted by this activity[a]
20.	Once refined standard operating procedures are established for NCRCG, US-CERT, National Operations Center, and Interagency Advisory Council (now the Crisis Action Team) organize and support the tabletop exercise to validate and refine interaction	1
21.	Support the development of a contact list of key public and private sector subject matter experts	1, 4, 5
22.	Once clear engagement thresholds are established, ensure that all interfacing organizations are aware of thresholds, levels of engagement, and implications of each	1
23.	Establish a mechanism for communicating real world implications of cyber incidents to DHS Public Affairs and the Public Affairs Working Group	1, 6
24.	Modify standard operating procedures to reflect any changes in Homeland Security Advisory System policy	1, 3
25.	Work to identify and contact NCRCG counterpart organizations within international partners	1, 2, 4
26.	Develop the capability to reach back to the private sector	1
27.	Move to develop public affairs messaging coordination among NCRCG, NCSD, the Information Technology Information Sharing and Analysis Center, and the Information Technology Sector Coordinating Council for both normal and emergency operations	1, 3, 6
28.	Engage in conversations with leadership to frame possible changes in rules for raising alert levels based on threats to cross-sector support structure	1, 3
29.	Establish processes, procedures, and physical means to communicate securely with NCRCG counterparts at a policy level	1, 2, 4
30.	Once Situation Awareness Toolset is established, arrange for appropriate centers to have it	1, 4
31.	In meeting with international participants, address coordination of standard operating procedures and concept of operations	1
32.	Work to establish secure communications with all international partners	1
33.	Procure Government Emergency Telecommunications Service cards for all NCRCG members	2
34.	Research secure cell phone capability for NCRCG members	2
35.	Work with a foreign computer emergency response team to cosponsor another foreign computer emergency response team into an intragovernmental incident response forum	2
36.	Install Critical Infrastructure Warning Information Network terminal in US-CERT	2
37.	Add redundant network support to US-CERT	2
38.	Procure 15 satellite phones	2
39.	Work to identify and organize a private sector counterpart for NCRCG with appropriate concepts of operations and standard operating procedures	2, 4, 5, 7
40.	Address public policy issues for industry incident response activities in cooperation with the industry and leadership	2
41.	Facilitate the development and implementation of cyber risk assessment methodologies across the information technology sector and in coordination with other sectors	2
42.	Coordinate standard operating procedures and concepts of operations with several ISACs	2, 3, 5

Activity identification number	DHS activity	Lesson(s) targeted by this activity[a]
43.	Submit request for continuity-of-operations space and establish continuity-of-operations plan	2
44.	Research alternatives to the Emergency Notification System	3
45.	Add dedicated support staff person to focus on processes and procedures	3
46.	Establish better e-mail connection during exercise to avoid spam filtering of injects	3, 5
47.	Execute semiannual tabletop exercise with accompanying education workshops focused on high-risk scenarios and cyber risk assessment	3, 5, 7, 8
48.	Coordinate standard operating procedures with US-CERT and the Information Technology and Communication ISACs	3, 4
49.	Transfer ticket tracking system over to an industry standard relational database tracking system for better correlation, analysis, and communication of incidents	3, 8
50.	Fill open spots with qualified personnel to gain bandwidth necessary to better address all aspects of US-CERT mission	3, 8
51.	Continue to expand network of informal and semiformal relationships with cyber-related associations and interest groups	4
52.	Forward request to require all federal computer emergency response teams to have secure communications, up to at least Secret	4, 7
53.	Request additional NCRCG support staff to address planning, correlation, and communication requirements	5
54.	Plan for significant pre-Cyber Storm II intelligence and law enforcement buildup exercise segment	5
55.	Complete permanent home of US-CERT, allowing classified operations to occur on-site	5
56.	Work to educate law enforcement on role and function of the NCRCG and establish sharing of cyber issues	5, 7
57.	Work to expedite tear-line policies (policies for organizing official documents so that unclassified information can be easily separated from classified information and disseminated)	5, 7
58.	Advocate inclusion of cyber public affairs in all exercises where appropriate	6
59.	Issue guidance to ISACs on a set of policies for cybersecurity-related public communications	6
60.	Establish baseline of public messaging based on cyber probable scenarios to include best channels for message delivery	6
61.	Develop comprehensive set of cyber scenarios to support exercises and planning	7
62.	Develop reporting process in coordination with reporting entities	8
63.	Participate in Internet Disruption Working Group tabletop exercise	8
64.	Plan and support cyber aspects of Top Officials 4 exercise	8
65.	Plan and execute Cyber Storm II	8
66.	Coordinate and develop situation report reporting process with National Operations Center and NCRCG	8

Source: GAO analysis of DHS data.

[a] The lessons are

Lesson 1: Interagency Coordination Groups

Lesson 2: Contingency Planning, Risk Assessment, and Roles and Responsibilities

Lesson 3: Integration of Incidents across Infrastructures

Lesson 4: Access to Information

Lesson 5: Coordination of Response Activities

Lesson 6: Strategic Communications and Public Relations

Lesson 7: Processes, Tools, and Technology

Lesson 8: The Exercise Program

Appendix III: GAO Analysis of DHS Efforts to Address Lessons from Cyber Storm I

Figure 1 shows, for each lesson learned during Cyber Storm I, the status of the activity as reported by DHS and whether the status could be validated by GAO. The activities are identified by number in appendix II.

Figure 1: Activity Status, as of June 2008, by Lesson

	Activities																														
Lessons	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
Lesson 1: Interagency Coordination Groups	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	0	0	0	0	0	0	>	+	>	
Lesson 2: Contingency Planning, Risk Assessment, and Roles and Responsibilities	+																+								0				0				+
Lesson 3: Integration of Incidents across Infrastructures	+													+			+	+	+					0			0	0					
Lesson 4: Access to Information	+			+	+		+									+	+		+		+				0				0	>			
Lesson 5: Coordination of Response Activities	+				+		+							+					+		+												
Lesson 6: Strategic Communications and Public Relations Plan																							+				0						
Lesson 7: Processes, Tools, and Technology	+				+		+						+		+				+														
Lesson 8: The Exercise Program	+				+		+																										

Key:

+ - Completed and validated

± - Completed but not validated

0 - Ongoing

> - Planned for the future

A blank box indicates the activity is not applicable to the lesson

Source: GAO analysis of DHS data.

	Activities																															
Lessons	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
Lesson 1: Interagency Coordination Groups																																	
Lesson 2: Contingency Planning, Risk Assessment, and Roles and Responsibilities	+	+	+	+	+	0	0	0	>	>																							
Lesson 3: Integration of Incidents across Infrastructures									>		+	+	+	+	>	>	>																
Lesson 4: Access to Information						0									>			0	0														
Lesson 5: Coordination of Response Activities						0			>				+	+						±	+	+	0	0									
Lesson 6: Strategic Communications and Public Relations Plan																									0	0	0						
Lesson 7: Processes, Tools, and Technology						0								+					0				0	0				+					
Lesson 8: The Exercise Program														+		>	>												+	+	+	+	+

Key:

+ - Completed and validated

± - Completed but not validated

0 - Ongoing

> - Planned for the future

A blank box indicates the activity is not applicable to the lesson

Source: GAO analysis of DHS data.

Appendix IV: Comments from the Department of Homeland Security

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

Homeland Security

August 22, 2008

Mr. David Powner
Director
Information Technology Management Issues
United States Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Powner:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO's) draft report entitled *CRITICAL INFRASTRUCTURE PROTECTION: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise* (GAO-08-825). Technical comments have been provided under separate cover.

The Department of Homeland Security's (DHS's) efforts to develop and refine procedures for addressing and tracking corrective actions have benefited from this GAO engagement. DHS fully agrees with GAO assertions that continuous progress and validation of exercise findings is essential to improving our Nation's cyber security, preparedness posture, and ensuring the best use of resources.

GAO states in its draft report that DHS addressed and completed 43 of the 66 corrective actions. The remaining 23 corrective actions included 16 items labeled "ongoing" and 7 items labeled "planned for the future." DHS addressed and completed over 66 percent of the total corrective actions at the time the GAO's report was drafted. Since the release of GAO's draft report, DHS completed additional items, raising the percentage of corrective actions completed to over 70 percent. A full breakdown of recent actions undertaken and discussion of their status is enclosed as Appendix A.

Recommendation: *Given the importance of continuously improving cyber exercises, we are making one recommendation to the Secretary of Homeland Security to direct the Assistant Secretary for Cybersecurity and Communications to ensure the scheduling and completion of the corrective actions addressing lessons learned during Cyber Storm I before conducting the next Cyber Storm exercise.*

Response: DHS concurs with the draft GAO report's recommendation and will continue to address actions related to Cyber Storm I findings. Many of the remaining corrective actions, however, are inherently long-term or ongoing in nature. Some corrective actions are within DHS's direct power to manage or perform, while others require extensive coordination with stakeholders.

Fulfilling the report's recommendation that the Department take action to ensure these remaining corrective actions are scheduled and completed before executing the next Cyber Storm exercise is dependent on various factors. DHS suggests that the remaining corrective actions are either: (1) *long-term* activities and are being incrementally addressed over time; (2) dependent upon *outside*

www.dhs.gov

stakeholder action; or (3) *ongoing*, addressed in different capacities over time, and a specific "end date" does not apply.

DHS appreciates the thorough analysis and very constructive points raised by the GAO draft report. To best capitalize on this analysis and recommendation, DHS plans an enhanced emphasis on how corrective action categories are defined for purposes of planning and integration into future exercises. DHS is willing to work with GAO as these efforts go forward. Finally, we ask that GAO modify the report to reflect the additional items the National Cyber Security Division (NCSD) has completed since the draft report's release.

Thank you again for the opportunity to comment on this draft report and we look forward to working with you on future homeland security issues.

Sincerely,

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Enclosure

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

David A. Powner, (202) 512-9286, or pownerd@gao.gov.

Staff Acknowledgments

In addition to the contact person named above, Colleen Phillips, Assistant Director; Neil Doherty; Nancy Glover; Jim MacAulay; Lee McCracken; and Jessica Waselkow 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