GAO

United States Government Accountability Office

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

June 2008

CRITICAL INFRASTRUCTURE PROTECTION

Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks

G A O

Accountability * Integrity * Reliability

G A O
Accountability·Integrity·Reliability

Highlights

CRITICAL INFRASTRUCTURE PROTECTION

Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks

Why GAO Did This Study

Technological advances have led to an increasing convergence of previously separate networks used to transmit voice and data communications. While the benefits of this convergence are enormous, such interconnectivity also poses significant challenges to our nation's ability to respond to major disruptions. Two operations centers—managed by the Department of Homeland Security's (DHS) National Communications System and National Cyber Security Division—plan for and monitor disruptions on voice and data networks. In September 2007, a DHS expert task force made three recommendations toward establishing an integrated operations center that the department agreed to adopt. To determine the status of efforts to establish an integrated center, GAO reviewed documentation, interviewed relevant DHS and private sector officials, and reviewed laws and policies to identify DHS's responsibilities in addressing convergence.

What GAO Recommends

GAO is recommending that the Secretary of Homeland Security complete (1) its strategic plan and (2) define tasks and milestones for completing remaining integration steps. DHS concurred with GAO's first recommendation. With regard to the second, DHS stated it supports integrating overlapping functions, but does not support merging the centers. However, there is strong evidence supporting the need to merge the centers to enhance incident response.

What GAO Found

DHS has taken the first of three steps toward integrating its centers that are responsible for planning for, monitoring, and responding to disruptions to the communications infrastructure, including voice and data networks, and the security of data and applications that use these networks. Specifically, in November 2007, it moved the operations center for communications infrastructure (NCC Watch) to office space adjacent to the center for data and applications (US-CERT). This close proximity allows the approximately 41 coordination center and 95 readiness team analysts to, among other things, readily collaborate on planned and ongoing activities. In addition, the centers have jointly acquired common software tools to identify and share physical, telecommunications, and cyber information related to performing their missions. For example, the centers use one of the tools to develop a joint "morning report" specifying their respective network security issues and problems, which is used by the analysts in coordinating responses to any resulting disruptions.

While DHS has completed the first integration step, it has yet to implement the remaining two steps. Specifically, although called for in the task force's recommendations, the department has not organizationally merged the two centers or invited key private sector critical infrastructure officials to participate in the planning, monitoring, and other activities of the proposed joint operations center. A key factor contributing to DHS's lack of progress in implementing the latter two steps is that completing the integration has not been a top DHS priority. Instead, DHS officials stated that their efforts have been focused on other initiatives, most notably the President's recently announced cyber initiative, which is a federal governmentwide effort to manage the risks associated with the Internet's nonsecure external connections. Nevertheless, DHS officials stated that they are in the process of drafting a strategic plan to provide overall direction for the activities of the National Communications System and the National Cyber Security Division. However, the plan is in draft and has been so since mid-2007. In addition, DHS officials could not provide a date for when it would be finalized. Consequently, the department does not have a strategic plan or related guidance that provides overall direction in this area and has not developed specific tasks and milestones for achieving the two remaining integration steps.

Until DHS completes the integration of the two centers, it risks being unable to efficiently plan for and respond to disruptions to communications infrastructure and the data and applications that travel on this infrastructure, increasing the probability that communications will be unavailable or limited in times of need.

_____

United States Government Accountability Office

Contents

Abbreviations

DHS	Department of Homeland Security
IT	information technology
NCC Watch	National Coordination Center Watch
NCC	National Coordination Center
NCS	National Communications System
NCSD	National Cyber Security Division
US-CERT	U.S. Computer Emergency Readiness Team

United States Government Accountability Office
Washington, DC 20548

June 26, 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

Effective voice and data networks and the information traveling on them
are essential to our ability as a nation to maintain public health and safety
during a catastrophic natural disaster, such as a hurricane, or a man-made
event, such as a terrorist attack. Technological advances in these networks
have led to an increasing consolidation of previously separate voice and
data networks into converged "next generation" networks that are capable
of transmitting both voice and data on a single network. Federal policies
assign two Department of Homeland Security (DHS) components—the
National Cyber Security Division (NCSD) and the National
Communications System (NCS)—responsibilities for planning for and
facilitating our nation's response to major disruptions on the
communications infrastructure, including voice and data networks.

In April 2007, DHS established a task force of subject matter experts to
study, among other things, whether there were opportunities to merge
NCSD and NCS operations. In September 2007, the task force made three
recommendations aimed at integrating aspects of NCSD and NCS
operations, namely those responsible for preparing for and responding to
network disruptions. DHS accepted the recommendations and, in doing
so, adopted a high-level approach for integrating the operations that
included the following steps:

- collocating the operations center of the national communications system
  that oversees the communications infrastructure, including voice and data
  networks—namely, the National Coordination Center Watch (NCC Watch)
  with the operations center of the NCSD that oversees the security of data
  and applications that use the communications infrastructure—called the
  U.S. Computer Emergency Readiness Team (US-CERT),

- developing an integrated operations center by merging NCC-Watch and US-CERT, and

- inviting private sector critical infrastructure officials to participate in the planning, monitoring, and other activities of the new operations center.

In response to your request, our objective was to determine the status of efforts to integrate NCSD and NCS activities to prepare for and respond to disruptions on converged voice and data networks. To accomplish this, we reviewed DHS documentation and interviewed DHS officials. To determine how these components were addressing convergence issues, we interviewed private sector stakeholders to obtain their perspectives on DHS's efforts to address convergence and reviewed laws and policies to identify DHS's responsibilities in addressing convergence. We conducted our work in the Washington, D.C. metropolitan area, from September 2007 to June 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. Details on our objective, scope, and methodology are in appendix I.

Results in Brief

DHS has taken the first of three steps toward integrating its centers responsible for planning for and monitoring the communications infrastructure, including voice and data networks, and the security of data and applications residing on these networks. Specifically, in November 2007, it moved the operations center for communications infrastructure—NCC Watch—to office space adjacent to the center for data and applications—US-CERT. This close proximity allows the approximately 41 coordination center and 95 readiness team analysts to, among other things, readily collaborate on planned and ongoing activities. In addition, the centers have jointly acquired common software tools to identify and share physical, telecommunications, and cyber information related to performing their missions. For example, the centers use one of the tools to develop a joint "morning report" specifying their respective security issues and problems, which is used by the analysts in coordinating responses to any resulting disruptions.

While DHS has completed this first integration step, it has yet to implement the other two. Specifically, the department has not organizationally merged the two centers or invited key private sector critical infrastructure officials to participate in the operation of the proposed joint center. DHS's lack of progress on the latter steps is

attributable, in part, to it not making integration a top DHS priority. Instead, its management efforts have been focused on other priorities, such as the President's recently announced cyber initiative. DHS officials stated that they are in the process of drafting a strategic plan to provide overall direction for the activities of NCS and NCSD, including completing the integration of the centers. However, the plan is in draft and has been so since mid-2007. In addition, DHS officials could not provide a date for when it would be finalized. Consequently, the department does not have a strategic plan or related guidance that provides overall direction in this area and has not developed specific tasks and milestones for achieving the remaining two integration steps.

Until DHS completes the integration of the two centers, it risks being unable to efficiently plan for and respond to disruptions to communications infrastructure and the data and applications that reside on this infrastructure, increasing the probability that communications will be unavailable or limited in times of need. Accordingly, we are recommending that the Secretary of DHS complete its strategic plan for NCSD and NCS and define the specific tasks and milestones for completing the remaining integration steps.

In commenting on a draft of this report, the department agreed with our first recommendation and did not support our second recommendation. With regard to the second recommendation, DHS stated that, while it supports further integration of overlapping functions, it does not support organizationally merging the centers at this time and added that the lack of a merger will not impact its ability to respond to incidents. We do not agree. To the contrary, there is strong evidence that DHS's ability to respond is negatively impacted by the use of separate centers, rather than a single integrated and merged entity. Our past work has shown that overlapping roles for incident response have adversely affected DHS's ability to prioritize and coordinate incident response activities.

Background

An effective communications infrastructure, including voice and data networks, is essential to our ability as a nation to maintain public health and safety during a catastrophic natural disaster, such as a hurricane, or a man-made event, such as a terrorist attack. Technological advances in these networks have led to a convergence of the previously separate networks used to transmit voice and data communications. These new networks—next generation networks—are capable of transmitting both voice and data on a single network and eventually will be the primary means for voice and data transmissions.

Converged voice and data networks have many benefits. For example, these networks use technology based on packet switching, which allows greater resiliency. Packet switching involves breaking a message into packets, or small chunks of data, and transferring the packets across a network to a destination where they are recombined. The resiliency of using a packet-switching network is due to the packet's ability to be transmitted over multiple routes, avoiding areas that may be congested or damaged. Conversely, conventional voice services use traditional telephone networks, which are based on circuit switching technology. Instead of breaking a message up into packets, circuit-switching uses a dedicated channel to transmit the voice communication. Once all of the channels are occupied, no further connections can be made until a channel becomes available. Figure 1 shows a comparison between packet switching and circuit switching.

Figure 1: Packet Switching vs. Circuit Switching
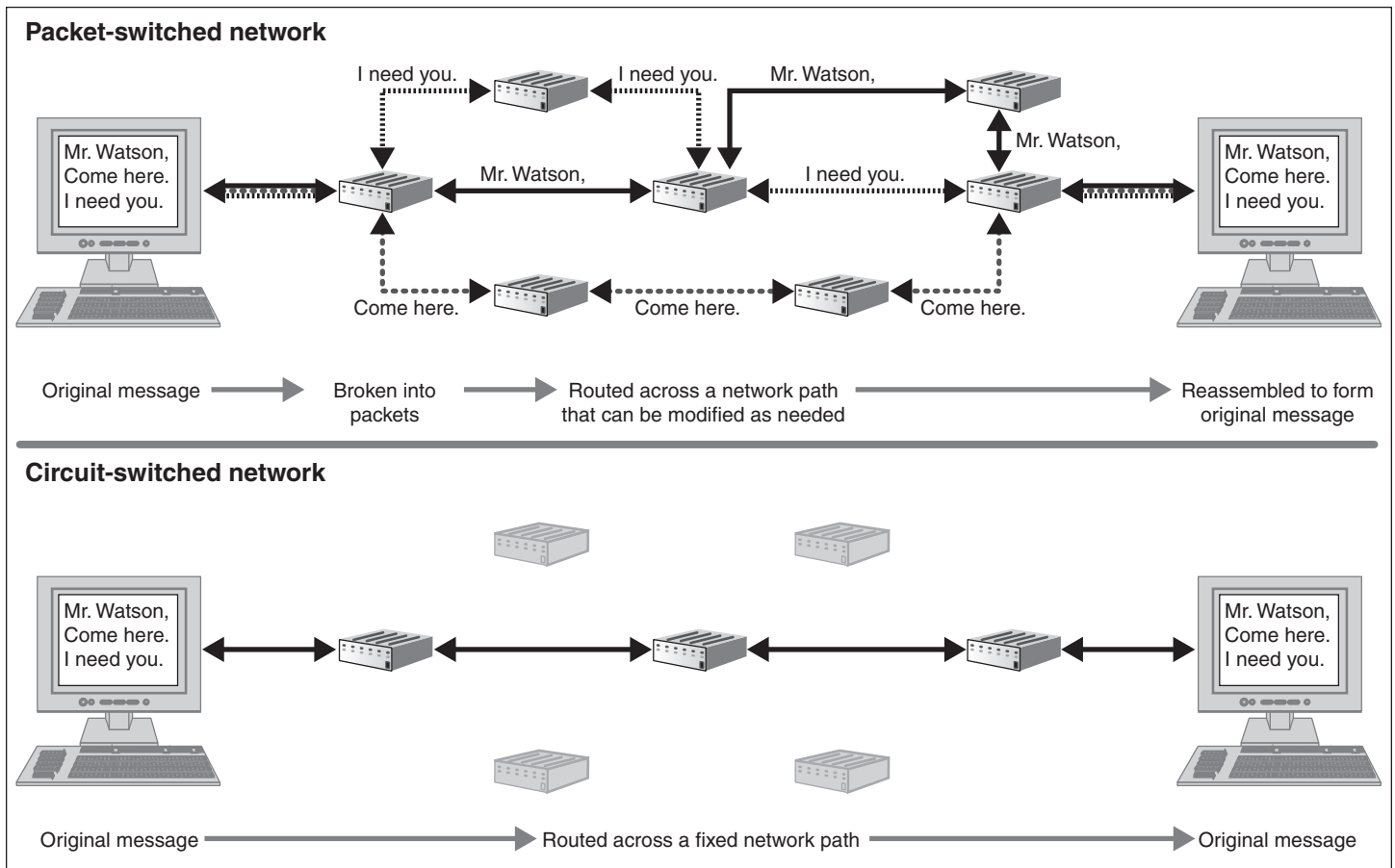
Source: GAO analysis; Art Explosion (images).

Converged networks, however, also pose certain technical challenges. For example, current national programs to provide priority voice services in an emergency are based primarily on voice or traditional telephone networks, which are circuit-switched. Implementing these networks on packet-switched networks is difficult because there is no uniformly accepted standard for providing priority service on a packet-switched network. Also, the Internet-based protocols used on packet-switched networks have vulnerabilities and in certain cases, packet-switched networks may be unreliable for emergency communications due to delays in transmission and loss of packets.

Federal Policies Provide for Critical Infrastructure Protection for Communications

Federal policies[1] call for the protection of essential public and private infrastructures, such as the electric power grid, chemical plants, and water treatment facilities that control the vital functions critical to ensuring our national economic security and public health and safety. These infrastructures, called critical infrastructures, also include communications infrastructure, such as voice and data communication networks. Federal policies also designate certain federal agencies as lead points of contact for each key critical infrastructure sector and assign responsibility for infrastructure protection activities and for coordination with other relevant federal agencies, state and local governments, and the private sector. (See app. II for a description of the sectors and the designated federal agencies.) DHS is the lead federal agency for both the telecommunications and information technology (IT) sectors. DHS is also designated 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 information systems.

As part of its responsibilities, DHS created the *National Infrastructure Protection Plan*[2] to coordinate the protection efforts of critical infrastructures. The plan recognizes the Internet as a key resource composed of assets within both the IT and the telecommunications sectors. It notes that the Internet is used by all critical infrastructure sectors to varying degrees and that it provides information and communications to meet the needs of businesses, government, and the other sectors. The *National Infrastructure Protection Plan* requires lead federal agencies for the critical infrastructure sectors to work with public and private sector stakeholders to develop sector-specific plans that address how the sectors' stakeholders will improve the security of their assets, systems, networks, and functions. We recently reported[3] on how comprehensively these sector-specific plans address the cyber security

---

[1]Homeland Security Presidential Directive Number 7 (Washington, D.C., December 2003), *National Infrastructure Protection Plan* (Washington, D.C., June 2006), *National Response Framework* (Washington, D.C., January 2008), and *National Strategy to Secure Cyberspace* (Washington, D.C., February 2003).

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

[3]GAO, *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-113 (Washington, D.C.: Oct. 31, 2007).

aspects of their sectors, including the plans for the IT and telecommunications sectors. We found that the plans varied in how sector stakeholders identified their cyber risks and developed plans to identify, respond to, and recover from a cyber attack. Accordingly, we recommended specific measures to help DHS strengthen the development, uniformity, and use of the plans.

DHS's Office of Cyber Security and Communications Is Responsible for Both Cyber and Telecommunications Security and Recovery

Federal policies[4] provide DHS the lead responsibility for facilitating a public-private response to disruptions to major communications infrastructure, such as voice and data networks. Within DHS, the responsibility is assigned to NCSD and NCS in the Office of Cyber Security and Communications. NCSD has responsibility for the security of data and applications and executes this duty via its operations center—US-CERT— while NCS has responsibility for the communications infrastructure that carries data and applications and carries out its duty through its coordination center, NCC, and its operations center, NCC Watch.

National Cyber Security Division

In June 2003, DHS created NCSD to serve as the national focal point for addressing cyber security issues. NCSD's mission is to secure cyberspace and America's cyber assets in cooperation with public, private, and international entities. The division carries out its mission via its US-CERT operations center, which is responsible for, among other things, analyzing and addressing cyber threats and vulnerabilities and disseminating cyber-threat warning information. In the event of a security issue or disruption affecting data and applications, US-CERT is to facilitate coordination of recovery activities with the network and security operations centers of owners and operators of these networks and with government officials (e.g., incident response teams) responsible for protecting government networks. NCSD is the government lead on a public/private partnership supporting US-CERT and serves as the lead for the federal government's cyber incident response through the National Cyber Response Coordination Group. This group is the principal federal interagency mechanism for coordinating the preparation for and response to

---

[4]See, for example, *National Strategy to Secure Cyberspace*, the *National Infrastructure Protection Plan*, the *Cyber Incident Annex* to the *National Response Framework*, and Homeland Security Presidential Directive 7.

significant cyber incidents, such as a major Internet disruption, and includes members from 19 federal departments and agencies.[5]

National Communications System

NCS is responsible for ensuring that communications infrastructure used by the federal government is available under all conditions—ranging from normal situations to national emergencies and international crises. The system does this through several activities, including a program that gives calling priority to federal executives, first responders, and other key officials in times of emergency. NCS was established by presidential direction[6] in August 1963 in response to voice communication failures associated with the Cuban Missile Crisis. Its role was further clarified through an executive order[7] issued in April 1984 that established the Secretary of Defense as the executive agent for NCS. In 2003, it was transferred to the responsibility of the Secretary of DHS.[8]

NCS is composed of members from 24 federal departments and agencies. Although it originally focused on "traditional" voice services via common carriers, NCS has now taken a larger role in Internet-related issues due to the convergence of voice and data networks. For example, it now helps manage issues related to disruptions of the Internet backbone (e.g., high-capacity data routes). NCC, which serves as the coordination component of NCS, is the point of contact with the private sector on issues that could affect the availability of the communications infrastructure. According to DHS, the center includes 47 members from major telecommunications organizations, such as Verizon and AT&T. These members represent 95 percent of the wireless and wire line telecommunications service providers and 90 percent of the Internet service provider backbone networks.

During a major disruption in telecommunications services, NCC Watch is to coordinate with NCC members in an effort to restore service as soon as

---

[5]They are the Central Intelligence Agency; the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Interior, Justice, State, Transportation, and the Treasury; the Director of National Intelligence; the Environmental Protection Agency; the Homeland Security Council; the National Security Agency; the National Security Council; the National Counterintelligence Executive; and the Office of Management and Budget.

[6]National Security Action Memorandum 252.

[7]Executive Order No. 12472, Section 1.e, April 3, 1984.

[8]Executive Order No. 12386, March 1, 2003.

possible. In the event of a major Internet disruption, it is to assist recovery efforts through its partnerships and collaboration with telecommunications and Internet-related companies. Using these partnerships, NCC has also created several programs that, in times of emergency, provide calling priority in to enable first responders and key officials at all levels to communicate using both landline phones and cellular devices.

Federal and Private Sector Experts Have Recommended a More Integrated Approach to Planning for and Responding to Disruptions on Converged Networks

Since February 2002, we, along with federal government and private sector experts, have examined the convergence of voice and data networks into next generation networks. All these experts recommend that federal agencies such as DHS adopt an integrated approach—including integrating their organizations—to planning for and responding to network disruptions.[9] In February 2002, before the formation of DHS, a White House advisory group recommended that the federal government develop such an approach.[10] Specifically, it found that timely information sharing was essential to effective incident response, that existing coordination within the government was ineffective and needed senior management attention, and that NCS should broaden its capabilities to include more IT industry expertise.

In March 2006, the National Security Telecommunications Advisory Committee, a presidential advisory group, also recommended that DHS develop an integrated approach to incident response on next generation networks and update priority communications programs to improve existing recovery abilities.[11] The committee recommended that DHS establish an inclusive and effective incident response capability that includes functions of the NCC and a broadened membership, including firms in the IT sector. The committee also stated that most new communications providers are not members of the NCC, were not easily

---

[9]GAO, *Internet Infrastructure: DHS Faces Challenges in Developing a Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006) and The President's National Security Telecommunications Advisory Committee, *Next Generation Network Task Force Report* (Washington, D.C., Mar. 28, 2006).

[10]White House Convergence Working Group, *Impact of Network Convergence on NS/EP Telecommunications: Initial Findings* and *FY02/FY03 Programmatic Recommendations Information Infrastructure Protection Assurance Group (IIPAG)* (Washington, D.C., July 2001).

[11]National Security Telecommunications Advisory Committee, *Next Generation Networks Task Force Report.*

accessible during an incident, and had not yet developed close working relationships with other industry stakeholders and the federal government.

In June 2006, we recommended that DHS improve its approach to dealing with disruptions by examining the organizational structure of NCSD and NCS in light of the convergence of voice and data networks. We found that DHS had overlapping responsibilities for incident response, which affected the ability of DHS to prioritize and coordinate incident response activities.[12]

Furthermore, in December 2006, the Telecommunications and Information Technology Information Sharing and Analysis Centers, composed of representatives of private telecommunications and IT companies, sent a letter to DHS asking that the department develop a plan to integrate critical infrastructure protection efforts including planning for and responding to disruptions. In a January 2007 written response signed by the Assistant Secretary for Cyber Security and Communications, DHS agreed with the importance of this effort and stated that developing a road map for integration was a priority.

Moreover, in April 2007, the two information sharing and analysis centers established a task force (referred to as a "tiger team" by DHS) with DHS that, among other things, identified overlapping responsibilities between NCC Watch and US-CERT in the following areas:[13]

- developing and disseminating warnings, advisories, and other urgent notifications;

- evaluating the scope of an event;

- facilitating information sharing;

- deploying response teams during an event;

- integrating cyber, communications, and emergency response exercises into operational plans and participation; and

---

[12]GAO-06-672.

[13]Industry Telecommunication and IT Sector Representatives, *Government Tiger Team Report and Recommendations for a Cyber Security and Communications Joint Operations Center* (Washington D.C., September 2007).

- the management of relationships with others, such as industry partners.

Consequently, the tiger team task force recommended merging the two centers to establish an integrated operations center and further recommended that DHS adopt a three-step approach to integration of the centers. The approach should include:

- moving NCC Watch to office space physically adjacent to US-CERT,

- developing an integrated operations center by merging US-CERT and NCC Watch, and

- inviting private sector critical infrastructure officials to join this new center.

In addition to these three steps, the task force also recommended specific actions to be taken in implementing them. For example, in developing an integrated operations center by merging NCC Watch and US-CERT, the task force recommended, among other things, that DHS (1) appoint a project manager to lead this effort; (2) develop policies and procedures that integrate operations and address overlapping responsibilities, including how the new center is to respond in an integrated manner to threats and incidents; and (3) establish performance measures to monitor progress. In addition, with regard to involving key private sector critical infrastructure officials in the new center, the task force recommended that the department also appoint a project manager to lead this effort. This effort would include seeking participation of appropriate private sector officials, identifying any potential legal issues to having these officials serve in the new center, and developing measures to monitor progress.

In September 2007, DHS approved the report, accepting the recommendations and adopting the three-step approach.

DHS Has Completed the First of Its Three-Step Integration Approach, but Has Yet to Implement the Remaining Steps

DHS has taken the first of three steps toward integrating NCSD and NCS by moving the two centers, NCC Watch and US-CERT, to adjacent office space in November 2007. This close proximity allows the approximately 41 coordination center and 95 readiness team analysts to, among other things, readily collaborate on planned and ongoing activities. In addition, the centers have jointly acquired common software tools to identify and share physical, telecommunications, and cyber information related to performing their missions. For example, the centers use one of the tools to develop a joint "morning report" specifying their respective security issues

and problems, which is used by the analysts in coordinating responses to any resulting disruptions.

While DHS has completed the first step, it has yet to implement the remaining two steps and supporting actions. Specifically, the department has not organizationally merged or integrated operation centers or completed any of the supporting actions. For example, the department has not hired a project manager, developed common operating procedures, or established progress measures. In addition, according to DHS officials, they have no efforts planned or underway to implement this step and associated actions.

With regard to involving key private sector officials to participate in the proposed joint center,[14] the department has not accomplished this step and supporting actions either. For example, it has not hired a project manager or sought participation of appropriate private sector officials to work at the new center. DHS officials told us they also have no efforts planned or underway to implement this step and its supporting actions.

A key factor contributing to DHS's lack of progress in implementing these steps is that completing the integration is not a top department priority. Instead, DHS officials stated that their efforts have been focused on other initiatives, most notably the President's recently announced cyber initiative, which is a federal governmentwide effort to manage the risks associated with the Internet's nonsecure external connections. Officials from DHS's Office of Cyber Security and Communications stated that they are in the process of drafting a strategic plan to provide overall direction for the activities of NCS and NCSD, including completing the integration of the centers. However, the plan is in draft and has been so since mid-2007. In addition, DHS officials could not provide a date for when it would be finalized. Consequently, the department does not have a strategic plan or related guidance that provides overall direction in this area and has not developed specific tasks and milestones for achieving the remaining two integration steps.

Until DHS completes the integration of these two centers, it risks being unable to efficiently plan for and respond to disruptions to communication infrastructure, including voice and data networks, and the information

---

[14]While officials from the telecommunications sector serve on the NCC and private sector IT firms have relationships with US-CERT, the tiger team task force recommended expanding membership of the new joint operations center to include officials from the other 16 critical infrastructure sectors.

traveling on these networks, increasing the probability that communications will be unavailable or limited in times of need.

Conclusions

While DHS has taken initial steps toward integrating the key centers that plan for and respond to disruptions to the communications infrastructure, including voice and data networks, and the data and applications on these networks, these offices are still not fully integrated as envisioned. Consequently, the risks associated with not having a fully integrated response to disruptions to the communications infrastructure remain. Effectively mitigating these risks will require swift completion of the integration. To do this will also require strong leadership to make the integration effort a department priority and to managing it accordingly, including completing the strategic plan and defining remaining integration tasks and milestones. To do less will continue to expose the nation's communications networks to continuing risk of inadequate response to an incident.

Recommendations for Executive Action

We are making two recommendations to the Secretary of Homeland Security to direct the Assistant Secretary for Cyber Security and Communications to

- Establish milestones for completing the development and implementation of the strategic plan for NCSD and NCS.

- Define specific tasks and associated milestones for establishing the integrated operations center through merging NCC Watch and US-CERT and inviting and engaging key private sector critical infrastructure officials from additional sectors to participate in the operations of the new integrated center.

Agency Comments and Our Evaluation

In written comments on a draft of this report (see app. III), signed by the Acting Director of DHS's Departmental Liaison Office, the department concurred with our first recommendation and stated it is taking steps to implement it. Specifically, the department said that as part of its effort to develop and implement a strategic plan, it intends to take into consideration, among other things, the recommendations of the various expert groups that have studied issues confronting DHS in this area and the lessons learned from collocating the two centers. Further, the department stated that this strategic planning also is to provide for integrating the centers' existing overlapping functions with the aim of increasing mission effectiveness.

With regard to our second recommendation, DHS stated that, while it supports further integration of overlapping functions, it does not support organizationally merging the centers at this point and added that the lack of a merger will not impact its ability to respond to incidents.

We do not agree. To the contrary, there is strong evidence that shows that DHS's ability to respond is negatively impacted by the use of separate centers, rather than a single integrated and merged entity. Specifically, our past work has shown that overlapping responsibilities for incident response have adversely affected DHS's ability to prioritize and coordinate incident response activities. For example, private-sector firms have reported that in responding to a critical incident, DHS made time-consuming and duplicative requests for information without identifying how this information would be beneficial in helping respond to the event. In addition, the DHS-commissioned expert task force on the subject recently reported that without an organizationally integrated center, the department will not have a comprehensive operating picture of the nation's cyber and communications infrastructure and thus not be able to effectively implement activities necessary to prepare, protect, respond, and recover this infrastructure. Further, our interviews with private-sector cyber and communications infrastructure executives performed as part of this engagement found that they also favor a merged organization that includes broad industry participation. This evidence calls for DHS to take a closer look at the issue of whether to merge the centers.

DHS also commented on the report's description of the roles and responsibilities of NCC and US-CERT. Specifically, DHS noted that our original characterization of NCC as dealing with voice systems and US-CERT with data systems was not totally accurate. Instead, DHS offered that a more accurate distinction would be that NCC deals with communication infrastructure, including voice and data networks, and US-CERT deals with the security of systems and data using the networks, which DHS commonly refers to as cyber situational awareness and response. We agree with this comment and have incorporated it in the report where appropriate.

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

We will send copies of this report to interested congressional committees, the Secretary of Homeland Security, 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 David A. Powner at (202) 512-9286 or at

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 major contributions to this report are listed in appendix IV.

David A. Powner
Director, Information Technology
 Management Issues

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the status of Department of Homeland Security (DHS) efforts to integrate the activities of its National Cyber Security Division (NCSD) and National Communications System (NCS) in preparing for and responding to disruptions in converged voice and data networks.

To accomplish this, we first analyzed pertinent laws, policies, and related DHS documentation (e.g., charters and mission statements) showing the responsibilities of NCSD and NCS, particularly with regard to the increasing convergence of voice and data networks. We also analyzed key studies on DHS's approach to managing convergence. We did this to identify key findings and recommendations pertinent to our objective. In particular, we focused on the *Industry-Government Tiger Team Report and Recommendations for a Cyber Security and Communications Joint Operations Center*, which recommended establishing an integrated operations center. DHS adopted the recommendations as part of its three-step approach to establish such a capability by (1) moving the National Coordination Center (NCC) Watch to office space physically adjacent to the US Computer Emergency Readiness Team (US-CERT), (2) developing an integrated operations center by merging NCC Watch and US-CERT, and (3) inviting private sector critical infrastructure officials to participate in this new center. We also interviewed DHS and industry officials who served on the tiger team task force and developed the report findings and recommendations.

To determine the status of DHS's efforts to integrate the centers, we analyzed department progress against the three steps specified in DHS's approach. We also obtained and analyzed plans and related documentation from DHS on its status in establishing an integrated operations center capability. In particular, we assessed department plans and related documentation on the status of collocating and merging the NCS and NCSD operations centers. In addition, we analyzed documentation on DHS's status in inviting key private sector infrastructure officials to join the operations of the new center. We also interviewed relevant officials in these organizations, including the managers of the National Coordination Center and the U.S. Computer Emergency Readiness Team, the Director of NCS, and the Acting Director of NCSD, to get their perspectives and to validate our understanding of their efforts to date. We also interviewed private sector officials—including the Chair of the Communications Information Sharing and Analysis Center and the President and Vice President of the IT Information Sharing and Analysis Center—to obtain their perspectives on DHS's progress in addressing convergence, including establishing the integrated center and to determine whether they had

received DHS invitations to participate in the operation of the integrated center.

Next, to identify gaps, we compared the state of DHS's progress against the task force recommendations adopted by DHS as part of its three step approach to integration. When gaps were identified, we also interviewed responsible DHS officials to determine any causes and their impact.

We conducted this performance audit in the Washington, D.C. metropolitan area from September 2007 to June 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: Critical Infrastructure Sectors

Table 1: Critical Infrastructure Sectors and Designated Sector-Specific Agencies

Sector	Sector-specific agency
Agriculture and food	Department of Agriculture, Department of Health and Human Services, Food and Drug Administration[a]
Banking and finance	Department of the Treasury
Chemical	Department of Homeland Security
Commercial facilities	Department of Homeland Security
Commercial nuclear reactors, materials, and waste	Department of Homeland Security
Critical Manufacturing	Department of Homeland Security
Dams	Department of Homeland Security
Defense industrial base	Department of Defense
Drinking water and water treatment systems	Environmental Protection Agency
Emergency services	Department of Homeland Security
Energy	Department of Energy
Government facilities	Department of Homeland Security
Information technology	Department of Homeland Security
National monuments and icons	Department of the Interior
Postal and shipping	Department of Homeland Security
Public health and health care	Department of Health and Human Services
Telecommunications	Department of Homeland Security
Transportation systems	Department of Homeland Security

Sources: 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 (including 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.

Appendix III: Comments from the Department of Homeland Security

Homeland Security

Mr. David A. Powner
Director
Information Technology Management Issues
United States Government Accountability Office
441 G Street, NW
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 GAO-08-607 entitled *Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks*. Technical comments have been provided under separate cover.

General Comments

1. This GAO report deals with the issue of the convergence of the communications and IT sectors by focusing primarily on the integration of the National Communications System's (NCS) National Coordinating Center (NCC) and the National Cyber Security Division's (NCSD) U.S. Computer Emergency Readiness Team (US-CERT). The fundamental concern is as technology converges into the Next Generation Network (NGN), this network continues to support national security and emergency preparedness (NS/EP) needs.

NCS and NCSD have established a variety of programs to ensure NS/EP communications are available during crisis and disasters when the general public's ability to communicate has been interrupted. The NCS is working to ensure priority services continue as industry converts to an Internet Protocol (IP) based transport network.

Current projections for NS/EP NGN priority voice over IP (VoIP) include an Initial Operational Capability (IOC) in 2012 while projections for NS/EP NGN broadband (data) priority services IOC is delayed due to receiving less funding than requested in FY 2008. Until these priority services are fielded, NS/EP priority voice and data communications over next generation IP networks will be unavailable to support Continuity of Government (COG) and Continuity of Operations (COOP) mission critical applications in times of crisis. This represents a greater risk to the ability of the Department to efficiently plan for and respond to voice and data network disruptions.

2. Much of this GAO report accepts the September 2007 recommendations of a "Tiger Team" to study the possibility of establishing a Cyber Security & Communications (CS&C) Joint Operations Center. The Tiger Team recommended merging US-CERT and NCC through a three-step approach. Given the importance of collaboration, US-CERT and NCC acted quickly to implement the first step by co-locating

www.dhs.gov

their facilities in November 2007. The co-location has ensured close coordination and improved information sharing between the two watches. The recent Estonia denial of service attack illustrated the capability of the NCC and US-CERT to jointly respond to an incident in an efficient and effective manner.

Co-locating these two centers has certainly increased the effectiveness of each, and further integration of certain complementary functions will likely yield better results. However, merging these two centers organizationally is not a top priority for a number of operational reasons:

- NCSD and NCS have focused time and resources on other initiatives, such as the Comprehensive National Cyber Initiative and the NGN (see General Comment #1 above).
- Although NCC and US-CERT have significant interdependencies which will increase as voice and data technologies converge, they have distinct missions, as described in General Comment #3 below.
- The increased coordination between the NCC and US-CERT has shown the uniqueness of their functions. This GAO report cites a list of overlapping responsibilities identified by the Tiger Team; however the execution of these responsibilities has proved to be different in several cases due to different subject matter, audiences, and missions (see Technical Comments, GAO Report page 11).
- Workspace classification level is another distinction between the two watches. US-CERT requires TS/SCI capability for its operations center, while NCS must maintain an operating space at SECRET and unclassified levels to coordinate with its industry partners. A merged watch would still require separate spaces to perform all of the necessary functions.

GAO's statement that without a merger, DHS risks not being able to efficiently plan for and respond to voice and data network disruptions is inaccurate. US-CERT and NCC have demonstrated through their collaborative planning and operational processes that there is little to no risk that a response cannot be planned and executed in times of need.

3. Throughout this report, the distinction between the NCC and the US-CERT is made by characterizing NCC as dealing with voice systems and US-CERT with data systems. This is not an accurate distinction. The mission of the NCC, as established by Executive Order 12472, is to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities under all conditions of crisis or emergency. Telecommunications services, as defined by the Federal Communications Commission, is "the transmission, emission, or reception of signals, signs, writing, images, sounds or intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio, visual or other electronic, electric, electromagnetic, or acoustically coupled means, or any combination thereof." This clearly encompasses more than just voice. A more accurate distinction between the NCC and US-CERT would be:

- NCC deals with communications infrastructure
- US-CERT deals with cyber situational awareness and response

To a large extent, the NCS deals with the infrastructure backbone and NCSD deals with the data and applications that ride on that backbone. This interdependence is illustrated by the fact that the internet backbone is owned largely by NCC industry members. Both NCC and US-CERT deal with all types of information transfer, whether it be voice, data, or multimedia. Indeed, as we move towards the NGN, the distinction between voice and data becomes less relevant. Certainly interdependencies between

2

communications infrastructure and cyber security will increase and the collaboration between NCC and US-CERT will create synergies and efficiencies, but there will always be a need for two distinct functions: ensure communications infrastructure supports NS/EP requirements and ensure the data and applications riding that infrastructure are secure.

Recommendation 1

- *establish milestones for completing the development and implementation of the strategic plan for NCSD and NCS, and*

Response

The NCS and NCSD concur with this recommendation and are taking steps to address it. However, the NCS and NCSD strategic plans, as an element of the CS&C strategic plan, should take into consideration not only the recommendations from the National Security Telecommunications Advisory Committee and the Tiger Team, but also lessons learned since co-locating NCC and US-CERT in November 2007. Co-location has provided a heightened awareness of the NCC's and US-CERT's distinct missions and operational requirements. The NCS and NCSD strategic plans should provide vision for communication collaboration while integrating overlapping functions that will increase the effectiveness of each organization.
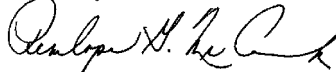
Recommendation 2

- *define specific tasks and associated milestones for establishing the integrated operations center through merging NCC and US-CERT and inviting and engaging key private sector critical infrastructure officials to participate in the operations of the new integrated center*

Response

As discussed in the General Comments, NCSD and NCS have distinct missions and operational requirements. Ensuring collaboration between NCC and US-CERT is paramount to successful response to national events. However, merging these two centers organizationally may not be practical or efficient for a number of operational reasons. NCS and NCSD support further integration of certain overlapping functions as appropriate, but they do not support organizationally merging the NCC and US-CERT at this time.

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,

Penelope G. McCormack
Acting Director
Departmental Audit Liaison Office

3

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, Gary Mountjoy (Assistant Director), Scott Borre, Camille Chaires, Neil Doherty, Vijay D'Souza, Nancy Glover, Lee McCracken, and Jeffrey Woodward 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