United States Government Accountability Office

Testimony

Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, March 26, 2014

CRITICAL INFRASTRUCTURE PROTECTION

Observations on Key Factors in DHS's Implementation of Its Partnership Approach

Statement of Stephen L. Caldwell, Director
Homeland Security and Justice

and

Gregory C. Wilshusen, Director
Information Security Issues

March 26, 2014

CRITICAL INFRASTRUCTURE PROTECTION

Observations on Key Factors in DHS's Implementation of Its Partnership Approach

GAO Highlights

Highlights of GAO-14-464T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Federal efforts to protect the nation's critical infrastructure from cyber threats has been on GAO's list of high-risk areas since 2003. Critical infrastructure is assets and systems, whether physical or cyber, so vital to the United States that their destruction would have a debilitating impact on, among other things, national security and the economy. Recent cyber attacks highlight such threats. DHS, as the lead federal agency, developed a partnership approach with key industries to help protect critical infrastructure.

This testimony identifies key factors important to DHS implementation of the partnership approach to protect critical infrastructure.

This statement is based on products GAO issued from October 2001 to March 2014. To perform this work, GAO reviewed applicable laws, regulations, and directives as well as policies and procedures for selected programs. GAO interviewed DHS officials responsible for administering these programs and assessed related data. GAO also interviewed and surveyed a range of other stakeholders including federal officials, industry owners and operators, industry groups, and cybersecurity experts.

What GAO Recommends

GAO has made recommendations to DHS in prior reports to strengthen its partnership efforts. DHS generally agreed with these recommendations and reports actions or plans to address many of them. GAO will continue to monitor DHS efforts to address these recommendations.

View GAO-14-464T. For more information, contact Stephen Caldwell at (202) 512-9610 or caldwells@gao.gov, or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

What GAO Found

GAO's prior work has identified several key factors that are important for the Department of Homeland Security (DHS) to implement its partnership approach with industry to protect critical infrastructure. DHS has made some progress in implementing its partnership approach, but has also experienced challenges coordinating with industry partners that own most of the critical infrastructure.

- **Recognizing and Addressing Barriers to Sharing Information.** Since 2003, GAO has identified information sharing as key to developing effective partnerships. In July 2010, GAO reported some barriers affecting the extent to which cyber-related security information was being shared between federal and industry partners. For example, industry partners reported concerns that sharing sensitive, proprietary information with the federal government could compromise their competitive advantage if shared more widely. Similarly, federal partners were restricted in sharing classified information with industry officials without security clearances. GAO recommended that DHS work with industry to focus its information-sharing efforts. DHS concurred and has taken some steps to address the recommendation, including sponsoring clearances for industry.

- **Sharing Results of DHS Assessments with Industry.** GAO has found that DHS security assessments can provide valuable insights into the strengths and weaknesses of critical assets and drive industry decisions about investments to enhance security. In a May 2012 report, GAO found that DHS was sharing the results of its assessments with industry partners, but these results were often late, which could undermine the relationship DHS was attempting to develop with these partners. GAO recommended that DHS develop time frames and milestones to ensure the timely delivery of the assessments to industry partners. DHS concurred and reported that it has efforts underway to speed the delivery of its assessments.

- **Measuring and Evaluating Performance of DHS Partnerships**. GAO's prior work found that taking a systematic approach to gathering feedback from industry owners and operators and measuring the results of these efforts could help focus greater attention on targeting potential problems and areas needing improvement. In an April 2013 report, GAO examined DHS's chemical security program and assessed, among other things, the extent to which DHS has communicated and worked with industry owners and operators to improve security. GAO reported that DHS had increased its efforts to communicate and work with industry to help them enhance security at their facilities. However, GAO found that DHS was not obtaining systematic feedback on its outreach. GAO recommended that DHS explore opportunities and take action to systematically solicit and document feedback on industry outreach. DHS concurred and reported that it had taken action to address the recommendation.

However, the cyber security of infrastructure remains on GAO's high-risk list and more needs to be done to accelerate the progress made. DHS still needs to fully implement the many recommendations on its partnership approach (and other issues) made by GAO and inspectors general to address cyber challenges.

Chairman Carper, Ranking Member Coburn, and Members of the Committee:

Thank you for the opportunity to discuss key factors in the Department of Homeland Security's (DHS's) implementation of partnership efforts to protect critical infrastructure from cyber attacks. Critical infrastructure is assets and systems, whether physical or cyber, that are so vital to the United States that their destruction would have a debilitating impact on, among other things, national security or the economy.[1]

Protecting the cybersecurity of our critical infrastructure is a top priority for the nation. For example, in February 2013, the President issued two policies—Executive Order 13636: *Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive PPD21: Critical Infrastructure Security and Resilience* —that aim to increase the overall security and resilience of U.S. critical infrastructure, including cyber security. Moreover, in February 2014, DHS partnered with the critical infrastructure community and established a voluntary program to strengthen critical infrastructure cybersecurity. The DHS Critical Infrastructure Cyber Community Voluntary Program is intended to be the coordination point within the federal government for partnering with critical infrastructure owners and operators interested in improving their cyber risk management processes.

We have recently testified that the federal government must address pressing challenges with cybersecurity and accelerate its progress in bolstering the cybersecurity posture of the nation.[2] As computer technology has advanced, our nation's critical infrastructures such as power distribution, water supply, telecommunications, and emergency services have become increasingly dependent on computerized information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is essential to protecting national security, economic prosperity, and public health and safety. We have reported that (1) cyber threats to critical infrastructure are evolving and growing, (2) cyber

[1]See 42 U.S.C. § 5195c(e).

[2]GAO, *Government Efficiency and Effectiveness: Views on the Progress and Plans for Addressing Government –wide Management Challenges*, GAO-14-436T (Washington, D.C.: March 12, 2014).

incidents affecting computer systems and networks continue to rise, and (3) the federal government continues to face challenges in a number of key aspects of its approach to protecting the nation's critical infrastructure.[3]

Since 2003, we have identified protecting systems supporting our nation's critical infrastructure—referred to as cyber-critical infrastructure protection, or cyber CIP—as a government-wide high-risk area, and we continued to do so in the most recent update to our high-risk list.[4] Since that time, the challenges and complexity of developing effective partnerships among the federal government, state and local governments, and industry owners and operators of our nation's critical infrastructure have remained. Our work has shown that trusted relationships are the centerpiece to the ability to share information—in particular information that private entities typically do not want to share and the barriers government faces to sharing. Further, improving information sharing is important, because information on threats and incidents experienced by others can help stakeholders identify trends, better understand the risks they face, and determine what preventive measures should be implemented. DHS's partnership approach is the way in which the federal and state governments and industry stakeholders develop, implement, and maintain a coordinated national effort to manage the risks to critical infrastructure.

My testimony today summarizes prior relevant work and provides our observations on three key factors that are important to DHS's implementation of its partnership approach to protect critical infrastructure from cyber attacks. Specifically, I will address the following factors: (1) recognizing and addressing barriers to sharing information, (2) sharing results of DHS assessments with industry and other stakeholders, and (3) measuring and evaluating the performance of DHS partnerships.

[3]GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2103).

[4]GAO's biennial high-risk list identifies government programs that have high vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges. We have designated federal information security as a high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure. See, most recently, GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: Feb.14, 2013).

This statement is based on reports we issued from October 2001 to March 2014 related to multiple aspects of DHS efforts to implement its partnership approach to protect critical infrastructure. To perform the work for our previous reports, among other things, we reviewed applicable laws, regulations, and directives as well as policies and procedures for selected programs to protect critical infrastructure. We also interviewed DHS officials responsible for administering these programs and obtained and assessed data on the conduct and management of DHS's security-related programs. We also interviewed and surveyed a range of other stakeholders, including federal officials, industry owners and operators, industry group officials, and cybersecurity experts. Further details on the scope and methodology for the previously issued reports are available within each of the published products.

We conducted the work on which this statement is based 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal law and policy have established roles and responsibilities for federal agencies to work with industry in enhancing the physical and cyber-security of critical government and industry infrastructures. For example, consistent with law, presidential policies stress the importance of coordination between the government and industry to protect the nation's cyber critical infrastructure. In addition, policies establish DHS as the focal point for the security of cyberspace—including analysis, warning, information sharing, vulnerability reduction, mitigation efforts, and recovery efforts for government and industry critical infrastructure and information systems. Federal policy also establishes critical infrastructure sectors, assigns federal agencies responsibilities over each sector (known as sector-specific agencies), and encourages industry involvement.

A fundamental component of DHS's efforts to protect and secure our nation's infrastructure is its partnership approach, whereby it engages in partnerships among government and industry stakeholders. In 2006, DHS

issued the *National Infrastructure Protection Plan* (NIPP),[5] which provides the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort.[6] The NIPP also outlines the roles and responsibilities of DHS with regard to critical infrastructure protection and resilience and sector-specific agencies—federal departments and agencies responsible for critical infrastructure protection and resilience activities in 16 critical infrastructure sectors—such as the dams, energy, and transportation sectors. Appendix I lists the 16 critical infrastructure sectors and their sector-specific agencies. The NIPP emphasizes the importance of collaboration, partnering, and voluntary information sharing among DHS and industry owners and operators, and state, local, and tribal governments. The NIPP also stresses a partnership approach between the federal and state governments, and industry stakeholders for developing, implementing, and maintaining a coordinated national effort to manage the risks to critical infrastructure.

Specific laws and directives have guided DHS's role in critical infrastructure protection, including the Homeland Security Act of 2002, as amended; Homeland Security Presidential Directive/HSPD-7; Presidential Policy Directive/PPD-21, which was issued on February 12, 2013; and Executive Order 13636, which was also issued on February 12, 2013. PPD-21 directs DHS to, among other things, coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure. PPD-21 also recognizes that DHS, in carrying out its responsibilities under the Homeland Security Act, evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security

[5]DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006). DHS issued the NIPP in response to the Homeland Security Act of 2002, as amended, and other authorities and directives. See, e.g., Pub. L. No. 107-296, § 201(d)(5), 116 Stat. 2135, 2146 (2002) (codified at 6 U.S.C. § 121(d)(5)). DHS updated the NIPP in January 2009 to include a greater emphasis on resiliency. See DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009). DHS further updated the NIPP, which is now called the National Plan, in December 2013. See DHS, *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

[6]According to DHS, in this context, resilience is the ability to adapt to changing conditions, and prepare for, withstand, and rapidly recover from disruptions. See DHS, Risk Steering Committee, *DHS Risk Lexicon* (Washington, D.C.: September 2010).

and resilience functions that are necessary for effective stakeholder engagement with all critical infrastructure sectors; integrates and coordinates federal cross-sector security and resilience activities; and identifies and analyzes key interdependencies among critical infrastructure sectors, among other things. Executive Order 13636 directs DHS to, among other things, develop a voluntary cybersecurity framework; promote and incentivize the adoption of cybersecurity practices; increase the volume, timeliness, and quality of cyber threat information sharing; and incorporate privacy and civil liberties protections into every initiative to secure our critical infrastructure.

Within DHS, the National Protection and Programs Directorate (NPPD) is responsible for working with public and industry infrastructure partners and leads the coordinated national effort to mitigate risk to the nation's infrastructure through the development and implementation of the infrastructure protection program. Using a partnership approach, NPPD works with owners and operators of the nation's infrastructure to develop, facilitate, and sustain strategic relationships and information sharing, including the sharing of best practices. NPPD also works with government and industry partners to coordinate efforts to establish and operate various councils intended to protect infrastructure and provide infrastructure functions to strengthen incident response.

Observations on Key Factors in DHS Implementation of Its Partnership Approach

Our prior work has found that DHS and its partners have taken a number of steps intended to improve the security of our critical infrastructure. However, we have also identified a number of additional steps DHS could take to further improve its partnerships aimed at protecting our critical infrastructure. Specifically, our work has identified three key factors that can affect the implementation of the partnership approach used by DHS: (1) recognizing and addressing barriers to sharing information; (2) sharing the results of DHS assessments with industry and other stakeholders; and (3) measuring and evaluating the performance of DHS's partnership efforts.

Recognizing and Addressing Barriers to Sharing Information

Addressing pervasive and sustained computer-based and physical attacks to systems and operations and the critical infrastructures they support depends on effective partnerships between the government and industry owners and operators of critical infrastructure. Recognizing and addressing barriers to information sharing includes, among other things, identifying barriers to sharing information with partners, understanding

information requirements, and determining partners' reasons for participating in voluntary programs.

- **Identifying barriers to industry sharing information with federal partners.** In a July 2010 report examining, among other things, government stakeholders' expectations for cyber-related, public-private partnerships we identified some barriers to industry's sharing of cyber threat information with federal partners.[7] We found that many of the government entities we contacted reported that industry partners were mostly meeting their expectations in several areas, including sharing timely and actionable cyber threat information, though the extent to which this was happening varied by sector. However, we found that federal officials also reported that improvements could be made. For example, while timely and actionable cyber threat and alert information was being received from industry partners, federal officials noted there were limits to the depth and specificity of the information provided by industry partners. Among other issues, we found that industry partners did not want to share their sensitive, proprietary information with the federal government. For example, information security companies had concerns that they could lose a competitive advantage by sharing information with the government if, in turn, this information was shared with those companies' competitors. In addition, despite special protections and sanitization processes, we found that industry partners were unwilling to agree to all of the terms that the federal government or a government agency requires to share certain information. On the basis of our findings, we recommended, among other things, that DHS, in collaboration with industry partners, use the results of our July 2010 report to continue to focus its information-sharing efforts on the most desired services. DHS concurred with this recommendation and described steps underway to address it, including the initiation of several pilot programs intended to enable the mutual sharing of cybersecurity information at various classification levels.

- **Identifying barriers to the government's sharing information with industry partners.** Federal efforts to meet the information-sharing expectations of industry partners are equally important in managing

[7]GAO, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*, GAO-10-628 (Washington, D.C.: July 15, 2010).

effective public-private partnerships to successfully protect cyber-reliant critical assets from a multitude of threats. In July 2010, we also examined industry partners' expectations for cyber-related, public-private partnerships and identified some barriers to the federal government's sharing of cyber threat information with its industry partners.[8] We reported that federal partners were not consistently meeting industry's information sharing expectations, including providing timely and actionable cyber threat information and alerts, according to industry partners we contacted at the time. We found that this was, in part, due to restrictions on the type of information that can be shared with industry partners. We reported that according to federal officials, DHS's ability to provide information is affected by restrictions that do not allow individualized treatment of one industry partner over another industry partner—making it difficult to formally share specific information with entities that are being directly affected by a cyber threat. In addition, we reported in July 2010 that because DHS has responsibility for serving as the nation's cyber analysis and warning center, it must ensure that its warnings are accurate.[9] Therefore, DHS subjects its products to a stringent review and revision process that can adversely affect the timeliness of its products—potentially adding days to the release if classified, law enforcement, or other information must be removed from the product. In addition, we found that federal officials are restricted to sharing classified information with industry officials in possession of appropriate security clearances and are hesitant to share sensitive information with industry partners, in part, because of the fear that sensitive information shared with corporations could be shared openly on a global basis. We recommended, and DHS concurred, that it should continue to focus information-sharing efforts on the most desired services, including providing security clearances. DHS reported that, among other things, it had instituted a clearance program for critical infrastructure representatives, such as industry partners, to enable their engagement in analysis of the most sensitive cybersecurity threat information.

[8]GAO-10-628.

[9]As part of its implementation of the cyberspace strategy and other requirements to establish cyber analysis and warning capabilities for the nation, DHS established the United States Computer Emergency Readiness Team (US-CERT) to help protect the nation's information infrastructure. US-CERT is the focal point for the government's interaction with federal and private sector entities 24 hours a day, 7 days a week, and is responsible for providing, among other things, cyber-related analysis, warning, information-sharing, major incident response, and national-level recovery efforts.

- **Understanding the information requirements of industry partners.** In our July 2012 report, we also found that federal officials did not have an adequate understanding of the specific private sector information requirements, which could have an adverse affect on federal partners' ability to meet industry partners' expectations. Specifically we found that multiple industry officials stated that federal partners could improve their methods of acquiring the type of information needed by the industry partners.[10] For example, more specific threat information could be focused on the technology being used by a particular entity or specify that a threat intended to target a particular entity, rather than including broad threat information and alerts. In addition, we reported that this more specific information would focus on the specific needs for each sector rather than all of the sectors getting the same information.

- **Determining why some industry partners do not participate in voluntary assessments.** DHS supports the development of the national risk picture by conducting vulnerability assessments and security surveys[11] to identify security gaps and potential vulnerabilities in the nation's most critical infrastructure. In a May 2012 report, we assessed the extent to which DHS had taken action to conduct these surveys and assessments among high-priority infrastructure, shared the results of these surveys and assessments with asset owners or operators, and assessed their effectiveness.[12] We found that various factors influence whether industry owners and operators of assets participate in these voluntary programs, but that DHS did not systematically collect data on reasons why some owners and operators of high-priority assets declined to participate in security surveys or vulnerability assessments. We concluded that collecting data on the reason for declinations could enhance the overall protection and resilience of those high-priority critical infrastructure

[10]GAO-10-628.

[11]DHS vulnerability assessments are conducted during site visits at individual assets and are used to identify security gaps and provide options for consideration to mitigate these identified gaps. DHS security surveys are intended to gather information on an asset's current security posture and overall security awareness. Security surveys and vulnerability assessments are generally asset-specific and are conducted at the request of asset owners and operators.

[12]GAO, *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments*, GAO-12-378 (Washington, D.C.: May 31, 2012).

assets crucial to national security, public health and safety, and the economy. We recommended, and DHS concurred, that it design and implement a mechanism for systematically assessing why owners and operators of high-priority assets decline to participate, and develop a road map, with time frames and milestones, for completing this effort. DHS stated that it had implemented a tracking system in October 2013 to capture data on the reason for declinations by owners and operators.

Although DHS reports that it has taken or begun to take action on the open recommendations discussed above, we have not verified DHS's progress implementing all of our recommendations. We will continue to monitor DHS's efforts to implement these recommendations.

Sharing Results of DHS Assessments with Industry and Other Stakeholders

Another important factor for DHS's implementation of its partnership approach is sharing information on the results of its security assessments and surveys with industry partners and other stakeholders.

- **Timely sharing of assessment results at the asset level.** DHS security surveys and vulnerability assessments can provide valuable insights into the strengths and weaknesses of assets and can help asset owners and operators that participate in these programs make decisions about investments to enhance security and resilience. In our May 2012 report, we found that, among other things, DHS shares the results of security surveys and vulnerability assessments with asset owners or operators.[13] However, we also found that the usefulness of security survey and vulnerability assessment results could be enhanced by the timely delivery of these products to the owners and operators and that the inability to deliver these products in a timely manner could undermine the relationship DHS was attempting to develop with these industry partners. Specifically, we reported that, based on DHS data from fiscal year 2011, DHS was late meeting its (1) 30-day time frame—as required by DHS guidance—for delivering the results of its security surveys 60 percent of the time and (2) 60-day time frame—expected by DHS managers for delivering the results of its vulnerability assessments—in 84 percent of the instances. DHS officials acknowledged the late delivery of survey and assessment results and said they were working to improve processes and

[13]GAO-12-378.

protocols. However, DHS had not established a plan with time frames and milestones for managing this effort consistent with standards for project management. We recommended, and DHS concurred, that it develop time frames and specific milestones for managing its efforts to ensure the timely delivery of the results of security surveys and vulnerability assessments to asset owners and operators. DHS stated that, among other things, it deployed a web-based information-sharing system for facility-level information in February 2013, which, according to DHS, has since resulted in a significant drop in overdue deliveries.

- **Sharing information with critical infrastructure partners at the sector level.** Critical infrastructures rely on networked computers and systems, thus making them susceptible to cyber-based risks. Managing such risk involves the use of cybersecurity guidance that promotes or requires actions to enhance the confidentiality, integrity, and availability of computer systems. In December 2011, we reported on cybersecurity guidance and its implementation and we found, among other things, that DHS and the other sector-specific agencies have disseminated and promoted cybersecurity guidance among and within sectors.[14] However, we also found that DHS and the other sector-specific agencies had not identified the key cybersecurity guidance applicable to or widely used in each of their critical infrastructure sectors. In addition, we reported that most of the sector-specific critical infrastructure protection plans for the sectors we reviewed did not identify key guidance and standards for cybersecurity because doing so was not specifically suggested by DHS guidance. Therefore, we concluded that given the plethora of guidance available, individual entities within the sectors could be challenged in identifying the guidance that is most applicable and effective in improving their security and that improved knowledge of the available guidance could help both federal and industry partners better coordinate their efforts to protect critical cyber-reliant assets. We recommended that DHS, in collaboration with government and industry partners, determine whether it is appropriate to have cybersecurity guidance listed in sector plans. DHS concurred with our recommendation and stated that it will work with its partners to determine whether it is appropriate to have cybersecurity guidance

[14]GAO, *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*, GAO-12-92 (Washington, D.C.: Dec. 9, 2011).

drafted for each sector and, in addition, would explore these issues with the cross-sector community.

- **Sharing certain information with critical infrastructure partners at the regional level.** Our work has shown that over the past several years, DHS has recognized the importance of and taken actions to examine critical infrastructure asset vulnerabilities, threats, and potential consequences across regions. In a July 2013 report, we examined DHS's management of its Regional Resiliency Assessment Program (RRAP)—a voluntary program intended to assess regional resilience of critical infrastructure by analyzing a region's ability to adapt to changing conditions, and prepare for, withstand, and rapidly recover from disruptions—and found that DHS has been working with states to improve the process for conducting RRAP projects, including more clearly defining the scope of these projects.[15] We also reported that DHS shares the project results of each RRAP project report with the primary stakeholders—officials representing the state where the RRAP was conducted—and that each report is generally available to certain staff, such as sector-specific agencies and protective security advisors[16] within DHS. However, we found that DHS did not share individual RRAP reports more widely with others in similar industry lines, including other stakeholders and sector-specific agencies outside of DHS. We also reported that DHS had been working to conceptualize how it can develop a product or products using multiple sources—including RRAP reports—to more widely share resilience lessons learned to its critical infrastructure partners, including federal, state, local, and tribal officials. DHS further reported using various forums, such as regional conferences or during daily protective security advisor contacts, to solicit input from critical infrastructure partners to gauge their resilience information needs. Due to DHS's ongoing efforts, we did not make a related recommendation in the report. However, we noted that through continued outreach and engagement with its critical infrastructure partners, DHS should be better positioned to understand their needs for information about resilience practices, which would in turn help clarify the scope of work

[15]GAO, *Critical Infrastructure Protection: DHS Could Strengthen the Management of the Regional Resiliency Assessment Program*, GAO-13-616 (Washington, D.C.: July 30, 2013).

[16]A protective security advisor is a DHS field representative. Among other things, they conduct RRAP projects.

needed to develop and disseminate a meaningful resilience information–sharing product or products that are useful across sectors and assets.

- **Sharing information with sector-specific agencies and state and local governments.** Federal sector-specific agencies and state and local governments are key partners that can provide specific expertise and perspectives in federal efforts to identify and protect critical infrastructure. In a March 2013 report, we reviewed DHS's management of the National Critical Infrastructure Prioritization Program (NCIPP)—which identifies and prioritizes a list of nationally significant critical infrastructure each year—to include how DHS worked with states and sector-specific agencies to develop the list.[17] We reported that DHS had taken actions to improve its outreach to sector-specific agencies and states in an effort to address challenges associated with providing input on nominations and changes to the NCIPP list. For example, in 2009, we reported that DHS revised its list development process to be more transparent and provided states with additional resources and tools for developing their NCIPP nominations. Furthermore, DHS provided on-site assistance from subject matter experts to assist states with identifying infrastructure, disseminated a lessons-learned document providing examples of successful nominations to help states improve justifications, and was more proactive in engaging sector-specific agencies in ongoing dialog on proposed criteria changes, among other efforts. However, we also found that most state officials we contacted continued to experience challenges with nominating assets to the NCIPP list using the consequence-based criteria developed by DHS. We reported that DHS officials told us that they recognized that some states are facing challenges participating in the NCIPP program and have taken additional steps to address the issue, including working to minimize major changes to the consequence-based NCIPP criteria; enhancing state participation; and working collaboratively with the State, Local, Tribal and Territorial Government Coordinating Council to develop a

[17]GAO, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, GAO-13-296 (Washington, D.C.: Mar. 25, 2013).

guide to assist states with their efforts to identify and prioritize their critical infrastructure.[18]

Furthermore, in our January 2014 report reviewing the extent to which federal agencies coordinated with state and local governments regarding enhancing cybersecurity within public safety entities, we determined that DHS shared cybersecurity-related information, such as threats and hazards, with state and local governments through various entities.[19] For example, we found that DHS collected, analyzed, and disseminated cyber threat and cybersecurity-related information to state and local governments through its National Cybersecurity and Communications Integration Center and through its relationship with the Multi-State Information Sharing and Analysis Center. In addition, we reported that DHS's State, Local, Tribal, and Territorial Engagement Office's Security Clearance Initiative facilitated the granting of security clearances to state chief information officers and chief information security officers which allowed these personnel to receive classified information about current and recent cyber attacks and threats. For example, we reported that, according to DHS officials, they have issued secret clearances to 48 percent of state chief information officers and 84 percent of state chief information security officers. Moreover, we reported that DHS provides unclassified intelligence information to fusion centers, which then share the information on possible terrorism and other threats and issue alerts to state and local governments. For example, in March

[18]DHS formed the State, Local, Tribal and Territorial Government Coordinating Council in April 2007 to strengthen sector partnership by bringing together experts from a wide range of professional disciplines that relate to critical infrastructure protection from all levels of government. The State, Local, Tribal and Territorial Government Coordinating Council supports geographically diverse partnerships to ensure state, local, tribal, and territorial officials play an integral role in national critical infrastructure protection and resiliency efforts.

[19]GAO, *Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology*, GAO-14-125 (Washington, D.C.: Jan. 28, 2014).

2013, a fusion center issued a situational awareness bulletin specific to public safety entities.[20]

Although DHS reports that it has taken or begun to take action on the open recommendations discussed above, we have not verified DHS's progress implementing all of our recommendations. We will continue to monitor DHS's efforts to implement these recommendations.

Measuring and Evaluating Performance of DHS Partnerships

Measuring and evaluating the performance of DHS partnerships—by among other things, obtaining and assessing feedback, evaluating why certain improvements are made, and measuring the effectiveness of partnerships and assessment—is another important factor in DHS's implementation of its partnership approach.

- **Obtaining and assessing feedback from industry partners.** Taking a systematic approach to gathering feedback from industry owners and operators and measuring the results of these efforts could help focus greater attention on targeting potential problems and areas needing improvement. In April 2013, we examined DHS's Chemical Facility Anti-Terrorism Standards (CFATS) program and assessed, among other things, the extent to which DHS has communicated and worked with owners and operators to improve security.[21] Specifically, we reported that DHS had increased its efforts to communicate and work with industry owners and operators to help them enhance security at their facilities since 2007. We found that as part of their outreach program, DHS consulted with external stakeholders, such as private industry and state and local government officials to discuss issues that affect the program and facility owners and operators. However, despite increasing its efforts to communicate with industry owners and operators, we also found that DHS had an opportunity to obtain systematic feedback on its outreach. We recommended that

[20]A fusion center is a collaboration of two or more federal, state, local, or tribal government agencies that combine resources, expertise, or information with the goal of maximizing the ability of such agencies to receive, gather, analyze, and disseminate information intended to detect, prevent, investigate, and respond to criminal or terrorist activity. DHS's Office of Intelligence and Analysis, through its State and Local Program Office, is responsible for coordinating federal support to fusion centers

[21]GAO, *Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, GAO-13-353 (Washington, D.C.: Apr. 5, 2013).

DHS explore opportunities and take action to systematically solicit and document feedback on facility outreach. DHS concurred with this recommendation and has actions underway to explore such opportunities to make CFATS-related outreach efforts more effective for all stakeholders.

- **Evaluating why facility-level improvements are made or not made.** According to the NIPP, the use of performance measures is a critical step in the risk management process to enable DHS to objectively and quantitatively assess improvement in critical infrastructure protection and resiliency at the sector and national levels. In our May 2012 report on DHS's efforts to conduct surveys and assessments of high-priority infrastructure assets and share the results, we found that, consistent with the NIPP, DHS has taken action to follow up with participants to gather feedback from asset owners and operators that participated in the program regarding the effect these programs have had on asset security.[22] However, we also found that DHS could consider using this follow-up tool to capture key information that could be used to understand why certain improvements were or were not made by asset owners and operators that have received surveys and assessments. For example, the follow-up tool could ask asset representatives what factors—such as cost, vulnerability, or perception of threat—influenced the decision to implement changes, either immediately or over time, if they chose to make improvements. We concluded that obtaining this information would be valuable to understanding the obstacles asset owners or operators face when making security investments. We recommended, and DHS concurred, that it consider the feasibility of expanding the follow-up program to gather and act upon data, as appropriate, on (1) security enhancements that are ongoing and planned that are attributable to DHS security surveys and vulnerability assessments and (2) factors, such as cost and perceptions of threat, that influence asset owner and operator decisions to make, or not make, enhancements based on the results of DHS security surveys and vulnerability assessments. DHS reported that it had modified the follow-up program to capture data on whether ongoing and planned security enhancements are attributable to security surveys and vulnerability assessments. Furthermore, DHS stated that it had also completed additional modifications to the follow-up tools to more

[22]GAO-12-378.

accurately capture all improvements to resilience as well as information on factors influencing owner and operator decisions to make or not make enhancements.

- **Measuring the effectiveness of sector-level partnerships.** Ensuring the effectiveness and reliability of communications networks is essential to national security, the economy, and public health and safety. In an April 2013 report, we found that while DHS has multiple components focused on assessing risk and sharing threat information, DHS and its sector partners do not consistently measure the outcome of efforts to improve cybersecurity at the sector level.[23] For example, we found that DHS and its partners had not developed outcome-based performance measures related to the cyber protection of key parts of the communications infrastructure sector. We concluded that outcome-based metrics related to communications networks and critical components supporting the Internet would provide federal decision makers with additional insight into the effectiveness of partner protection efforts at the sector level. We recommended that DHS collaborate with its partners to develop outcome-oriented measures for the communications sector. DHS concurred with our recommendation and stated that it is working with industry to develop plans for mitigating risks that will determine the path forward in developing outcome-oriented performance measures for cyber protection activities related to the nation's core and access communications networks.

- **Measuring the effectiveness of regional-level assessments.** Similarly, in our July 2013 report examining DHS's management of its RRAP program, we found that DHS had taken action to measure efforts to enhance security and resilience among facilities that participated in these regional-level assessments, but faced challenges measuring the results associated with these projects.[24] Consistent with the NIPP, DHS performs periodic follow-ups among industry partners that participate in these regional assessments with the intent of measuring their efforts to make enhancements arising out of these surveys and assessments. However, we found that DHS did not

[23]GAO, *Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts*, GAO-13-275 (Washington, D.C.: Apr. 3, 2013).

[24] GAO-13-616.

measure how industry partners made enhancements at individual assets that participate in a RRAP project contribute to the overall results of the project. DHS officials stated at the time that they faced challenges measuring performance within and across RRAP projects because of the unique characteristics of each, including geographic diversity and differences among assets within projects. However, we concluded that DHS could better position itself to gain insights into projects' effects if it were to develop a mechanism to compare facilities that have participated in a RRAP project with those that have not, thus establishing building blocks for measuring its efforts to conduct RRAP projects. We recommended that DHS develop a mechanism to assess the extent to which individual projects influenced partners to make RRAP-related enhancements. DHS concurred with our recommendation and reported that it had actions underway to review alternatives, including possibly revising its security survey and vulnerability assessment follow-up tool, to address this recommendation.

Although DHS reports that it has taken or begun to take action on the open recommendations discussed above, we have not verified DHS's progress implementing all of our recommendations. We will continue to monitor DHS's efforts to implement these recommendations.

Concluding Remarks

In closing, the federal government has taken a variety of actions that are intended to enhance critical infrastructure cybersecurity. Improving federal capabilities—through partnerships with industry, among other things—is a step in the right direction, and effective implementation can enhance federal information security and the cybersecurity and resilience of our nation's critical infrastructure. However, more needs to be done to accelerate the progress made in bolstering the cybersecurity posture of the nation. The administration and executive branch agencies need to fully implement the hundreds of recommendations made by GAO and agency inspectors general to address cyber challenges. Until then, the nation's most critical federal and private sector infrastructure systems will remain at increased risk of attack from our adversaries.

Chairman Carper, Ranking Member Coburn, and members of the committee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

For information about this statement please contact Stephen L. Caldwell, at (202) 512-9610 or CaldwellS@gao.gov, or Gregory C. Wilshusen, at (202) 512-6244 or WilshusenG@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Other individuals making key contributions to this work included Edward J. George, Jr., Assistant Director; Michael W. Gilmore, Assistant Director; Hugh Paquette, Analyst-in-Charge; Jose Cardenas; Tom Lombardi; and Erin McLaughlin.

Appendix I: Critical Infrastructure Sectors

This appendix provides information on the 16 critical infrastructure (CI) sectors and the federal agencies responsible for sector security. The *National Infrastructure Protection Plan* (NIPP) outlines the roles and responsibilities of the Department of Homeland Security (DHS) and its partners—including other federal agencies. Within the NIPP framework, DHS is responsible for leading and coordinating the overall national effort to enhance protection via 16 critical infrastructure sectors. Consistent with the NIPP, Presidential Decision Directive/PPD-21 assigned responsibility for the critical infrastructure sectors to sector-specific agencies (SSAs).[1] As an SSA, DHS has direct responsibility for leading, integrating, and coordinating efforts of sector partners to protect 10 of the 16 critical infrastructure sectors. Seven other federal agencies have sole or coordinated responsibility for the remaining 6 sectors. Table 1 lists the SSAs and their sectors.

[1] Issued on February 12, 2013, Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*, purports to refine and clarify critical infrastructure related functions, roles, and responsibilities across the federal government, and enhance overall coordination and collaboration, among other things. Pursuant to Homeland Security Presidential Directive/HSPD-7 and the *National Infrastructure Protection Plan*, DHS had established 18 critical infrastructure sectors. PPD-21 subsequently revoked HSPD-7, and incorporated 2 of the sectors into existing sectors, thereby reducing the number of critical infrastructure sectors from 18 to 16. Plans developed pursuant to HSPD-7, however, remain in effect until specifically revoked or superseded.

Table 1: Critical Infrastructure Sectors and Sector-Specific Agencies (SSA)

Critical infrastructure sector	SSA(s)[a]
Food and agriculture	Department of Agriculture[b] and the Department of Health and Human Services[c]
Defense industrial base[d]	Department of Defense
Energy[e]	Department of Energy
Government facilities	Department of Homeland Security and the General Services Administration
Health care and public health	Department of Health and Human Services
Financial services	Department of the Treasury
Transportation systems	Department of Homeland Security and the Department of Transportation[f]
Water and wastewater systems[g]	Environmental Protection Agency
Commercial facilities Critical manufacturing Emergency services Nuclear reactors, materials, and waste Dams Chemical	Department of Homeland Security Office of Infrastructure Protection[h]
Information technology Communications	Office of Cyber Security and Communications[i]

Source: Presidential Policy Directive/PPD-21

[a]Presidential Policy Directive/PPD-21, released in February 2013, identifies 16 critical infrastructure sectors and designates associated federal SSAs. In some cases co-SSAs are designated where those departments share the roles and responsibilities of the SSA.

[b]The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[c]The Food and Drug Administration is the Department of Health and Human Services component responsible for food other than meat, poultry, and egg products and serves as the co-SSA.

[d]Nothing in the NIPP impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commanders of military forces, or military command and control procedures.

[e]The energy sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

[f]Presidential Policy Directive/PPD- 21 establishes the Department of Transportation as co-SSA with the Department of Homeland Security (DHS) for the transportation systems sector. Within DHS, the U.S. Coast Guard and the Transportation Security Administration are the responsible components.

[g]The water sector includes drinking water.

[h]The Office of Infrastructure Protection is the DHS component responsible for the commercial facilities; critical manufacturing; emergency services; nuclear reactors, materials, and waste; dams; and chemical sectors.

[i]The Office of Cyber Security and Communications is the DHS component responsible for the information technology and communications sectors.