



441 G St. N.W.
Washington, DC 20548

November 18, 2013

The Honorable Mary Landrieu
Chairman
The Honorable Dan Coats
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
United States Senate

The Honorable John Carter
Chairman
The Honorable David Price
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

CRITICAL INFRASTRUCTURE: Assessment of the Department of Homeland Security's Report on the Results of Its Critical Infrastructure Partnership Streamlining Efforts

A fundamental component of the Department of Homeland Security's (DHS) efforts to protect and secure our nation's critical infrastructure (CI) is partnerships among public and private stakeholders.¹ In 2006, DHS issued the *National Infrastructure Protection Plan* (NIPP),² which provides the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort.³ The NIPP also outlines the roles and responsibilities of DHS with regard to critical infrastructure protection and resilience and sector-specific agencies (SSA)—federal departments and agencies responsible for critical infrastructure protection and resilience activities in critical infrastructure sectors—such as the

¹Critical infrastructure is assets and systems, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. See 42 U.S.C. § 5195c(e).

²DHS, *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).

³According to DHS, resiliency 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). DHS developed the risk lexicon to provide a common set of official terms and definitions to ease and improve the communication of risk-related issues for DHS and its partners. The NIPP risk management framework is a planning methodology that outlines the process for setting goals and objectives; identifying assets, systems, and networks; assessing risk based on consequences, vulnerabilities, and threats; implementing protective programs and resiliency strategies; and measuring performance and taking corrective action.

dams, energy, and transportation sectors. Because the private sector owns the majority of the nation's critical infrastructure—banking and financial institutions, commercial facilities, and energy production and transmission facilities, among others—it is vital that the public and private sectors work together to protect these assets and systems. The NIPP emphasizes the importance of collaboration, partnering, and voluntary information sharing among DHS and private sector asset owners and operators, and state, local, and tribal governments.

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

In 2011, a report of the Senate Committee on Appropriations accompanying H.R. 2017—the fiscal year 2012 spending bill for DHS—noted that the department's budget request stated that NPPD would streamline various methods and processes for coordination and information sharing with industry partners through NIPP management, Critical Infrastructure and Key Resources coordination, and SSA management.⁴ The committee report directed NPPD to provide a report, not later than 60 days after enactment of the bill, on the results from a thorough review of all efforts related to five areas: (1) coordinating and executing plans; (2) implementing performance metrics; (3) sustaining systemic communication; (4) executing SSA functions; and (5) providing education, training, and outreach.⁵ The committee report further stated that GAO shall review the results of the NPPD report and related efforts of the streamlining process no later than 60 days after receiving the report to determine the extent to which NPPD's efforts were designed to ensure mission clarity, useful and actionable work products, efficacy of planning and information sharing, and that cost savings were achieved where possible.⁶ Although H.R. 2017 was not enacted into law, DHS received its appropriation through the Consolidated Appropriations Act, 2012.⁷ Explanatory text in the conference report accompanying the Consolidated Appropriations Act acknowledged that NPPD is to provide a report regarding the results of a review to streamline the processes for coordination and information sharing with industry partners, and that GAO is to conduct an evaluation of the effort, as stated in the Senate report.⁸

⁴See S. Rep. No. 112-74, at 108-09 (2011) (accompanying H.R. 2017, the Department of Homeland Security Appropriations Bill, 2012).

⁵Id.

⁶Id. at 109.

⁷Pub. L. No. 112-74, Div. D, 125 Stat. 786, 943 (2011).

⁸See H.R. Rep. No. 112-331, at 986 (2011) (Conf. Rep.). Pursuant to the explanatory text in the conference report, the language and allocations contained in Senate Report 112-74 should be complied with and carry the same emphasis as the language included in the explanatory text, unless specifically addressed to the contrary in the conference report or explanatory text. Id. at 944. Accordingly, with enactment of the Consolidated Appropriations Act (enacted December 23, 2011), NPPD was, in effect, directed to report to both the House and Senate Committees on Appropriations no later than 60 days following enactment.

In response to the Senate committee report language, on August 27, 2013, DHS provided us with its *2011-2012 National Critical Infrastructure Protection and Resilience Annual Report* (National Annual Report), dated August 19, 2013.⁹ This report was accompanied by a nine-page annex that maps relevant sections of the National Annual Report to the five areas listed in the Senate committee report and provides explanatory language where necessary.

This report summarizes the results of our review of DHS's submission. Specifically, this report discusses our assessment of DHS's response to the Senate report and related efforts of NPPD's streamlining process to determine the extent to which these efforts were designed to ensure mission clarity, useful and actionable work products, efficacy of planning and information sharing, and that cost savings were achieved where possible.

To conduct our work, we analyzed the DHS annex and the referenced content in the 2011-2012 National Annual Report to determine the extent to which NPPD's streamlining efforts were designed to ensure mission clarity; useful and actionable work products; efficacy of planning and information sharing; and that cost savings were achieved where possible, consistent with the language from the Senate report. In so doing, we reviewed the DHS annex and the referenced content in the 2011-2012 National Annual Report to determine the extent to which NPPD discussed the results of its efforts to streamline the processes for coordination and information sharing with industry partners. We did so within the context of the five areas outlined for NPPD in the Senate report as discussed above. We conducted this performance audit from September 2013 to November 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results

DHS's August 2013 response does not discuss NPPD efforts to streamline the processes for coordination and information sharing with industry partners. As a result, we were unable to assess the extent to which NPPD's streamlining efforts were designed to ensure mission clarity, useful and actionable work products, efficacy of planning and information sharing, and that cost savings were achieved where possible. Our analysis of DHS's response showed that DHS provided information on NPPD efforts, organized by the five areas discussed in the Senate committee report, to coordinate and share information with its partners and the results of some of those efforts. However, DHS did not provide information about any NPPD efforts to streamline the processes for coordination and information sharing; rather, DHS described actions NPPD has taken or plans to take that are related to each of the five areas, and examples of how its actions are intended to benefit coordination and information sharing. Table

⁹The Homeland Security Act, as amended, requires the Secretary of Homeland Security to report annually to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives, and to other appropriate congressional committees with jurisdiction over CI, on the comprehensive assessments carried out by the Secretary of the CI for each sector, evaluating threat, vulnerability, and consequence, and include, if applicable, actions or countermeasures recommended or taken to address issues identified in the assessments. See 6 U.S.C. § 121(d)(25). The National Annual Report is intended to fulfill this reporting requirement and assess the performance of the critical infrastructure protection and resilience community in implementing the NIPP. The 2011-2012 National Annual Report presents data, observations, and findings regarding critical infrastructure risks and protection activities from May 1, 2010, through December 31, 2011.

1 summarizes information included in DHS’s response, and with respect to DHS’s streamlining efforts, in each of the five areas outlined in the Senate committee report.

Table 1: DHS’s Response to the Mandate in Each of the Five Areas Outlined in the Senate Committee Report

Area noted in Senate committee report	Summary of response	Response provided with respect to streamlining
Coordinating and Executing Plans	According to DHS’s response, NPPD’s Office of Infrastructure Protection (NPPD/IP) coordinates and executes plans with various stakeholders (e.g., CI owners and operators). DHS stated that the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI) seeks to ensure that activities conducted to meet the requirements of the NIPP are developed and executed considering foreseeable risks to critical infrastructure. DHS further reported that, as part of CIRMEI, DHS intends to develop short-term and long-term steps that NIPP partners can take to address certain risks and opportunities related to CI that are to enhance the coordination and execution of risk-management plans.	No
Implementing Performance Metrics	DHS’s response stated that, as part of CIRMEI, outcome-based metrics were developed and implemented to better assess the current state of critical infrastructure protection and resilience. DHS highlighted a number of these metrics and related outcomes, and noted that there is much work to be done in defining a set of metrics against which all partners and NPPD/IP can measure progress in critical infrastructure protection and resilience.	No
Sustaining Systemic Communication	DHS reported that partnership, programmatic, and information sharing mechanisms are in place to provide systemic communication with and among CI stakeholders. To demonstrate that these mechanisms are in place, DHS noted, for example, the number of public and private members in the NIPP Sector Partnership and the number of fusion centers that joined the Critical Infrastructure Information Sharing Environment.	No
Executing Sector-Specific Agency Functions	According to DHS’s response, SSAs function through five primary program areas: effective planning and activity integration, education and training, information sharing and communication, exercises, and assessment and mitigation. DHS highlighted performance metrics that NPPD uses to evaluate SSA functions. For example, NPPD maintains a metric to assess whether stakeholders have an understanding of critical infrastructure risks and interdependencies. According to DHS, NPPD analyses found that stakeholders understand that critical infrastructure risks and interdependencies exist, but further assessment is needed to understand the extent of the stakeholders’ understanding.	No

Area noted in Senate committee report	Summary of response	Response provided with respect to streamlining
Providing Education, Training and Outreach	DHS stated that NPPD/IP offers a variety of education and training resources to CI stakeholders. For example, DHS reported that in 2011, the critical infrastructure information sharing environment hosted 28 educational events and reached approximately 17,500 stakeholders. DHS also stated that NPPD/IP conducts outreach to share information and intelligence, develop partnerships, and conduct vulnerability and security assessments, among other things. DHS's response also noted that the successful implementation of the NIPP partnership framework, for example, demonstrates the value of NPPD/IP outreach efforts.	No

Source: GAO analysis of DHS information.

For example, DHS's annex to the National Annual Report includes a section called "Coordinating and Executing Plans," which generally describes who NPPD's partners are and ways that NPPD coordinates and executes plans with these various stakeholders. In addition, the annex describes steps NPPD plans to take that are intended to improve the coordination and execution of plans. However, neither the section in the annex nor the references to materials in the National Annual Report describe steps NPPD has taken or plans to take to streamline efforts associated with the coordination and execution of plans and how, if at all, coordination and information sharing might be affected. In another example, DHS's annex includes a section entitled "Implementing Performance Metrics" that describes NPPD's efforts to establish performance metrics intended to "describe the desired 'end state' for national critical infrastructure protection and resilience," which, according to DHS, are intended to enable the NIPP partners to better assess the current state of critical infrastructure protection and resilience. However, neither DHS's discussion of performance metrics nor the metrics displayed showed how metrics might be applied with regard to streamlining the processes for coordination and information sharing with industry partners, or how coordination and information sharing might be affected.

NPPD officials stated that they agreed that the submission provided by DHS does not discuss NPPD efforts to streamline the processes for coordination and information sharing with industry partners. They further acknowledged that the submission was not responsive to the concerns reflected in the Senate committee report and the conference report. These officials informed us that they are currently working with your committees to address this issue, noting that they intend to provide information on their plans to streamline the processes for coordination and information sharing with industry partners within the context of the broader review and update efforts associated with the NIPP, as directed by Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*.¹⁰ According to DHS's June 2013 Federal Register Notice, PPD-21 is intended to enhance the security and resilience of critical infrastructure by clarifying the roles and responsibilities across the federal government and establishing a more effective partnership with owners and operators and state, local, tribal, and territorial entities.¹¹ The successor to the NIPP is to include a description of functional relationships within DHS and

¹⁰On February 12, 2013, President Obama signed Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*. PPD-21 explicitly calls for DHS to take several actions to implement the directive, including the development of a successor to the NIPP.

¹¹78 Fed. Reg. 34,112 (June 6, 2013).

across the federal government related to critical infrastructure security and resilience and any changes to the sector partnership resulting from the evaluation of the existing public-private partnership model.¹² As these initiatives are under way or planned, we could not assess the extent to which they will identify efforts to streamline the processes for coordination and information sharing with industry partners, as directed in the related Senate committee report language.

Agency Comments

We provided a draft of this report to DHS for review and comment. In its written comments, which are reproduced in enclosure I, DHS stated that it has taken substantial steps toward streamlining information and enhancing activities in the areas referenced in the Senate committee report, but concurred that the report provided by DHS falls short of fully capturing and describing these actions. DHS also described actions it has taken, is taking, or plans to take to provide a framework for streamlining methods and processes for coordinating information sharing with industry partners and the other issues identified in the Senate committee report. DHS also provided technical comments which we incorporated where appropriate.

- - - - -

We are sending copies of this report to the appropriate congressional committees and the Secretary of Homeland Security. This report is also available at no charge on the GAO website at <http://www.gao.gov>. Should you or your staff have questions concerning this report, please contact me at (202) 512-9610 or Caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were John Mortin (Assistant Director), Jeffrey Fiore, Tracey King, and Hugh Paquette.



Stephen L. Caldwell
Director
Homeland Security and Justice Issues

Enclosure

¹²Id.

Enclosure I: Comments from the Department of Homeland Security

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



**Homeland
Security**

November 12, 2013

Stephen L. Caldwell
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-14-100R, "CRITICAL INFRASTRUCTURE: Assessment of the Department of Homeland Security's Report on the Results of Its Critical Infrastructure Partnership Efforts"

Dear Mr. Caldwell:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

While the Department has taken substantial steps toward streamlining information sharing and enhancing activities in the areas referenced in the Senate Appropriations Committee (SAC) report request, the Department concurs that the provided National Protection and Programs Directorate (NPPD) report falls short of fully capturing and describing these actions. The Department has reorganized divisions, altered programmatic activities, and reviewed current and past NPPD Office of Infrastructure Protection outreach efforts to federal, state, and local governments and private-sector partners since the SAC report request.

With the release of Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," in February 2013, review and update of the critical infrastructure outreach activities has been a primary focus for the Department. The result of these efforts includes the revision and update of significant policies, such as the National Infrastructure Protection Plan (NIPP), which establishes the core foundation for information sharing with the private sector. The NIPP will include a Call to Action that specifies actions the Federal Government can take in collaboration with the critical infrastructure community to inform, guide, and advance the national effort (e.g., joint planning efforts, evaluating achievement of goals, information sharing, and technical assistance, training, and education).

In addition, the NIPP will include supplemental tools to assist members of the partnership in risk management and resilience activities, such as information sharing (e.g., how to connect to the national critical infrastructure operating centers that facilitate information sharing and situational awareness for physical and cyber infrastructure). The 2014 Sector-Specific Plans will describe sector-specific implementation of NIPP 2013 and will address the Senate issues in greater detail. The NIPP 2013 will be submitted to the White House by November 30, 2013, and is scheduled for publication by December 31, 2013. The work done to produce this and the other PPD-21

deliverables provides a framework for streamlining methods and processes for coordinating information sharing with industry partners and the other issues identified in Senate Report 112-74.

Additional progress will be made during calendar year 2014, as NPPD implements a formal communication plan to socialize the NIPP to a broad range of critical infrastructure owners and operators. This outreach will include an education and training program for those who are not as familiar with the NIPP 2013 (e.g., state and local government infrastructure owners and operators, small businesses) to better understand how they can participate in critical infrastructure security and resilience activities. NPPD, as the lead implementer for critical infrastructure activities within the Department, welcomes interim opportunities to provide additional information to address the original request with the intent of better clarifying the progress made in these areas.

Again, thank you for the opportunity to review and provide comments on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,



Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

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

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 website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

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

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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

