United States Government Accountability Office

GAO

Report to Congressional Requesters

March 2013

CRITICAL INFRASTRUCTURE PROTECTION

DHS List of Priority Assets Needs to Be Validated and Reported to Congress

GAO

Accountability * Integrity * Reliability

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-13-296, a report to congressional requesters

Why GAO Did This Study

In October 2012, Hurricane Sandy caused widespread damage across multiple states and affected millions of people. Threats to critical infrastructure are not limited to natural disasters, as demonstrated by the terrorist attacks of September 11, 2001. Originally developed by DHS in 2006, and consistent with the Implementing Recommendations of the 9/11 Commission Act of 2007, the NCIPP identifies and prioritizes nationally significant critical infrastructure each year. However, Members of Congress and some state officials have raised questions about changes DHS has made to its approach for creating the list and the impact of these changes.

GAO was asked to review DHS management of the program. GAO assessed the extent to which DHS has (1) changed its criteria for developing the list, identified the impact, if any, of these changes, and validated its approach, (2) worked with states and SSAs to develop the list, and (3) reported to Congress on the NCIPP. GAO, among other things, reviewed laws, DHS policies and procedures; analyzed the lists from 2007 through 2012; and interviewed DHS, SSA, and state homeland security officials selected based on their involvement with the program and geographic diversity. The interviews are not generalizable but provide insights.

What GAO Recommends

GAO recommends that DHS commission an external peer review and develop an approach to verify that the annual reports are provided to the requisite committees of Congress. DHS concurred with the recommendations.

View GAO-13-296. For more information, contact Stephen Caldwell at (202) 512-8777 or caldwells@gao.gov.

March 2013

CRITICAL INFRASTRUCTURE PROTECTION

DHS List of Priority Assets Needs to Be Validated and Reported to Congress

What GAO Found

The Department of Homeland Security (DHS) has made several changes to its criteria for including assets on the National Critical Infrastructure Prioritization Program (NCIPP) list of the nation's highest-priority infrastructure, but has not identified the impact of these changes or validated its approach. In 2009, DHS changed the criteria to make the list entirely consequence based—that is, based on the effect of an event on public health and safety, and economic, psychological, and government mission impacts. Subsequent changes introduced specialized criteria for some sectors and assets. For example, infrastructure that has received a specific, credible threat, but otherwise does not meet NCIPP criteria, may be included on the list. DHS's changes to the NCIPP criteria have changed the composition of the NCIPP list, which has had an impact on users of the list, such as the Federal Emergency Management Agency. However, DHS has not reviewed the impact of changes on users nor validated its approach to developing the list. While the change to an entirely consequence-based list created a common approach to identify infrastructure and align the program with applicable laws and the *National Infrastructure Protection Plan*, recent criteria changes to accommodate certain sectors and assets represent a departure from this common approach, which could hinder DHS's ability to compare infrastructure across sectors. Program officials noted they would like to validate the NCIPP, but they have not yet submitted a proposal to DHS management. An independent peer review—a best practice in risk management—would better position DHS to reasonably assure that the NCIPP list identifies the nation's highest-priority infrastructure.

To develop the list, DHS has consulted with both states and sector specific agencies (SSA)—federal agencies responsible for protection and resiliency efforts among individual critical infrastructure sectors, such as energy, transportation, and dams. Since changing the NCIPP criteria in 2009, DHS has taken proactive steps to help states nominate assets to the list. These steps include providing on-site assistance, minimizing changes to the criteria, conducting outreach to encourage participation in an NCIPP working group (which includes SSAs), and providing explanations of why nominated assets do not make the list. DHS recognizes that states, in particular, face challenges—such as resource and budgetary constraints—associated with nominating assets, and has taken actions to address these challenges and reduce the burden on states.

GAO could not verify that DHS is meeting statutory requirements 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 on the NCIPP list. DHS officials prepared documents that generally contained information consistent with statutory reporting requirements, but they were uncertain whether they had been delivered to the committees because they do not have records to verify they were delivered. An approach to verify the delivery of the required reports, such as documenting or recording the transactions, would better position DHS to ensure that it is in compliance with its statutory reporting requirements and that it provides the committees with the information needed to perform oversight of the program.

Contents

Tables

Figures

Abbreviations

DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FMD	foot-and-mouth disease
FMFIA	Federal Managers' Financial Integrity Act of 1982
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSPD	Homeland Security Presidential Directive
IASD	Infrastructure Analysis and Strategy Division
MSA	metropolitan statistical area
NCIPP	National Critical Infrastructure Prioritization Program
NIPP	*National Infrastructure Protection Plan*
NPPD	National Protection and Programs Directorate
PPD	Presidential Policy Directive
PSA	Protective Security Advisor
PSCD	Protective Security Coordination Division
SHSP	State Homeland Security Program
SSA	sector-specific agency
UASI	Urban Area Security Initiative

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 25, 2013

The Honorable Thomas R. Carper
Chairman
The Honorable Tom Coburn, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Patrick Meehan
Chairman
Subcommittee on Cybersecurity, Infrastructure Protection
and Security Technologies
Committee on Homeland Security
House of Representatives

The Honorable Susan M. Collins
United States Senate

In October 2012, the remnants of Hurricane Sandy caused widespread damage across multiple states and affected millions of people. Damage included flooding in the nation's financial center that affected major transportation systems and caused widespread and prolonged power outages. The damage and resulting chaos disrupted government and business functions alike, producing cascading effects far beyond the location of these events. Threats against critical infrastructure are not limited to natural disasters, as demonstrated by the terrorist attacks of September 11, 2001, and the 2005 suicide bombings in London, where terrorists disrupted the city's transportation system, which resulted in a breakdown of its mobile telecommunication infrastructure. In March 2007, we reported that our nation's critical infrastructure—assets and systems, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a negative or debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters—continue to be vulnerable to a wide variety of threats.[1] Because the private sector owns the vast

[1] GAO, *Critical Infrastructure: Challenges Remain in Protecting Key Sectors*, GAO-07-626T (Washington, D.C.: Mar. 20, 2007).

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 identify, prioritize, and protect these assets and systems.

In 2006, in accordance with section 201 of the Homeland Security Act of 2002, as amended,[2] and other authorities and directives,[3] the Department of Homeland Security (DHS) issued the *National Infrastructure Protection Plan* (NIPP), which provides the overarching approach for integrating the nation’s critical infrastructure protection and resiliency activities into a single national effort.[4] The NIPP sets forth a risk management framework and details the roles and responsibilities of DHS and other federal, state, regional, local, tribal, territorial, and private sector partners implementing the NIPP, and emphasizes the importance of collaboration and partnering with and among the various partners.[5] For example, the NIPP outlines the roles and responsibilities of sector-specific agencies (SSA)—the various federal departments and agencies that are responsible for critical infrastructure protection and resiliency activities—in 18 sectors, such as

[2] See 6 U.S.C. § 121.

[3] See, e.g., Homeland Security Presidential Directive/HSPD-7 (Washington, D.C.: Dec. 17, 2003).

[4] DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006). DHS updated the NIPP in January 2009 to include resiliency. See DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009). According to DHS, resiliency is the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

[5] According to DHS, 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.

the chemical, dams, energy, and transportation sectors.[6] Appendix I lists the SSAs and their sectors.

Consistent with the NIPP, provisions of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) amended title II of the Homeland Security Act of 2002 by requiring the Secretary of DHS to establish and maintain a national database of systems and assets determined to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States, any state, or any local government, as otherwise determined appropriate for inclusion by the Secretary.[7] In addition, the 9/11 Commission Act required the Secretary of DHS to establish and maintain a single prioritized list of systems and assets included in the national database that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects.[8] The 9/11 Commission Act also required that DHS 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 on, among other things, any significant challenges in compiling the database or list and, if appropriate, the extent to which the database or list has been used to allocate federal funds to prevent, reduce, mitigate, or respond to acts of terrorism.[9]

[6] See Homeland Security Presidential Directive/HSPD-7 (Dec. 17, 2003). According to the NIPP, sectors are defined as a logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The 18 sectors are defined within the context of Homeland Security Presidential Directive/HSPD-7, which directed DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across critical infrastructure sectors. Seventeen sectors were initially established pursuant to HSPD-7. DHS established an 18th sector—critical manufacturing—pursuant to the directive in 2008. Although Presidential Policy Directive/PPD-21, issued February 12, 2013, revokes HSPD-7 and realigns the 18 sectors into 16 critical infrastructure sectors, it also provides that plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

[7] See 6 U.S.C. § 124*l*(a)(1).

[8] See 6 U.S.C. § 124*l*(a)(2).

[9] See 6 U.S.C. § 124*l*(d).

Originally developed in 2006, the National Critical Infrastructure Prioritization Program (NCIPP) uses a tiered approach to identify nationally significant critical infrastructure each year based on the consequences associated with the disruption or destruction of those critical infrastructure.[10] Within DHS, the Office of Infrastructure Protection in the National Protection and Programs Directorate (NPPD) is responsible for infrastructure protection and resilience. The Infrastructure Analysis and Strategy Division (IASD),[11] within the Office of Infrastructure Protection, manages the NCIPP.[12] IASD coordinates a voluntary effort with states and other partners to identify, prioritize, and categorize high-priority critical infrastructure as either level 1 or level 2 based on the consequences to the nation in terms of four factors—fatalities, economic loss, mass evacuation length, and degradation of national security.[13] According to the NIPP, the list identifies nationally significant critical infrastructure that DHS can use to enhance decision making, including implementing Federal Emergency Management Agency (FEMA)

[10] Prior to DHS implementing provisions of the 9/11 Commission Act related to the establishment of the database and prioritized list of systems and assets, agencies, including DHS, collected and maintained infrastructure information through independent data collection tools including the National Asset Database, Risk Analysis and Management for Critical Asset Protection, the Constellation/Automated Critical Asset Management System, and the Vulnerability Identification Self-Assessment Tool, as well as sector-specific datasets such as the U.S. Army Corps of Engineers' National Inventory of Dams. During this time period, the lists DHS developed were referred to as the Tier 1/Tier 2 Program.

[11] In May 2012, we reported that the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) coordinated the NCIPP. HITRAC is an office within IASD. See GAO, *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments*, GAO-12-378 (Washington, D.C.: May 31, 2012).

[12] Our past work has shown that DHS leverages existing regulatory frameworks, where applicable, to implement the NIPP with its security partners within and across the 18 sectors and identify critical infrastructure security overlaps and gaps to enhance and supplement existing sector regulations. GAO, *Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities*, GAO-11-537R (Washington, D.C.: May 19, 2011), and *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened*, GAO-10-772 (Washington, D.C.: Sept. 23, 2010).

[13] According to DHS, the overwhelming majority of the assets and systems identified through the NCIPP are categorized as level 2. Only a small subset of assets meet the level 1 consequence threshold—those whose loss or damage could result in major national or regional impacts similar to the impacts of Hurricane Katrina or the September 11, 2001, attacks.

homeland security grant programs and federal incident management planning and response efforts.

In recent years, Members of Congress and some state officials have raised questions as to whether and why DHS has changed its approach for assigning assets to the list, with some assets either dropping off the list or being assigned to a new risk level. In addition, they have raised questions about the effect changes to the program may have had on states and SSAs that work with DHS to develop the list, as well as those that use the list.[14] Given the importance of the NCIPP list to various aspects of DHS's critical infrastructure protection and resiliency efforts, you asked that we examine DHS's management of the program. Specifically, we assessed the extent to which DHS has

- changed its criteria for developing the NCIPP list; identified the impact, if any, of these changes; and validated its approach;
- worked with states and SSAs to develop the NCIPP list; and
- reported to Congress on the NCIPP.

To address our first objective, we reviewed applicable laws, regulations, and directives as well as Office of Infrastructure Protection policies and procedures for developing and managing the NCIPP list, and assessed the impact of changes on how the list is used. We also obtained and assessed Office of Infrastructure Protection data on the program by identifying and analyzing the distribution of high-priority assets included on the finalized NCIPP lists by sector and state from fiscal years 2007 through 2012. We used our analysis to select 8 of 18 sectors—the banking and finance, defense industrial base, chemical, energy, transportation systems, agriculture and food, government facilities, and dams sectors.[15] We selected these sectors to obtain a mix of sectors that

[14] In May 2012, we reported that DHS officials attributed challenges to managing some voluntary critical infrastructure programs to "significant" changes to the NCIPP list from year to year. See GAO-12-378.

[15] On February 12, 2013, the President issued Presidential Policy Directive/PPD-21, which, among other things, reduced the number of critical infrastructure sectors from 18 to 16. The directive also revoked HSPD-7 but provided that plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded. This does not affect our review because we began and conducted the bulk of our work prior to the release of this directive.

experienced the largest and smallest percentage change in the distribution of assets on the NCIPP list between fiscal years 2009 and 2011 because of program changes that DHS made during this period.[16] The information from our analysis of these sectors is not generalizable to the universe of all sectors. However, it provides valuable insights into yearly changes in the distribution of assets on the NCIPP list among a diverse group of sectors. We then compared the results of our analysis with various criteria, including the NIPP; DHS guidelines shared with state and federal partners on the processes and methodologies used to identify assets to be included on the NCIPP list; and *Standards for Internal Control in the Federal Government*.[17] We interviewed IASD officials in Washington, D.C., responsible for administering the NCIPP program. We also conducted a sensitivity analysis with the FEMA Urban Area Security Initiative (UASI) grant risk formula—which uses NCIPP data, among other information—to determine how, if at all, the changes to the list could affect allocations for this grant. We discussed the sources of the data and quality assurance procedures with Office of Infrastructure Protection and FEMA officials and determined that the data were sufficiently reliable to provide a general overview of the program; we reported on data limitations in prior work and have noted them in this report, where applicable.[18]

To address our second objective, we interviewed 10 SSA officials in Washington, D.C., representing the 8 selected sectors to determine whether DHS worked with these SSAs to develop the list, and if so, the

[16] Because of the challenges encountered with changes DHS made to the NCIPP criteria in 2009, the fiscal year 2010 NCIPP list was not approved by the Assistant Secretary for Infrastructure Protection and therefore not finalized or used.

[17] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999). Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982 (FMFIA), provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to FMFIA, the Office of Management and Budget issued Circular A-123, revised December 21, 2004, to provide the specific requirements for assessing the reporting on internal controls. Internal control standards and the definition of internal control in Circular A-123 are based on GAO's *Standards for Internal Control in the Federal Government*.

[18] GAO-12-378.

extent to which consultations occurred. Specifically, DHS was the SSA for 4 of the sectors—the chemical, dams, government facilities, and transportation systems sectors.[19] The Departments of Energy, Defense, and the Treasury were the SSAs for 3 sectors—the energy, defense industrial base, and banking and finance sectors, respectively. Two SSAs, the Department of Agriculture and the Food and Drug Administration, share responsibility for the agriculture and food sector. In addition, we contacted officials representing homeland security offices in 15 states to obtain their views on DHS efforts to work with them to develop the NCIPP list. We selected these states because they contained a range in the number of assets on the NCIPP list.[20] We also selected the 15 states based on their distribution in each of the 9 Protective Security Advisor (PSA) regions—the Office of Infrastructure Protection's field office designations for managing its PSA program—and selected at least 1 state in each of the 9 regions.[21] As of December 2012, DHS has deployed 91 PSAs in all 50 states, Puerto Rico, and the nation's capital region to, among other things, conduct outreach with state and local partners and asset owners and operators who participate in DHS's voluntary critical infrastructure protection and resiliency efforts. Furthermore, we spoke with 9 of the 91 PSAs—at least 1 from each PSA region consistent with our state selection criteria—to discuss their contributions to the NCIPP list, how they use the list to prioritize their activities, and actions NCIPP management has taken to solicit feedback regarding the program. The information from our interviews with SSA officials, state homeland security officials, and PSAs are not generalizable to the universe of state and federal infrastructure partners. However, they provide valuable insights into the Office of Infrastructure Protection efforts to develop and manage its NCIPP list.

[19] Two DHS components are the SSAs for the transportation systems sector: the Transportation Security Administration and the U.S. Coast Guard.

[20] For the purposes or our review, we selected states that contained a mix of smaller, medium-sized, and larger numbers of assets on the list. The precise number of assets on the NCIPP list is information that DHS designated "for official use only." We have not included this information in this report so that we could publicly present the results of our work.

[21] During the course of our review, DHS realigned the PSA regions to match the standard federal regions (i.e., the 10 FEMA regions). However, for the purpose of our review, which began prior to the realignment, the PSA regions were the National Capital Region, Great Lakes Area, Gulf Coast Area, Mid-Atlantic Area, Midwest Area, Northeast Area, Northwest Area, Southeast Area, and Southwest Area.

To address our third objective, we reviewed the statutory requirement that DHS 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 on the national asset database and prioritized critical infrastructure list. We reviewed documents on the national asset database and prioritized critical infrastructure list that were intended to meet statutory reporting requirements to determine if these efforts were consistent with relevant statutory provisions and *Standards for Internal Control in the Federal Government*.[22] We also interviewed Office of Infrastructure Protection officials to discuss efforts to report to Congress. Appendix II discusses our objectives, scope, and methodology in greater detail.

We conducted this performance audit from May 2012 to March 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.

Background

Pursuant to the Homeland Security Act of 2002, as amended, DHS has responsibility for the protection of the nation's critical infrastructure.[23] Within DHS, the Office of Infrastructure Protection is responsible for critical infrastructure protection and resilience and leads the coordinated national effort to mitigate risk to the nation's critical infrastructure, which includes working with public and private sector infrastructure partners.[24] The Office of Infrastructure Protection also has the overall responsibility for coordinating implementation of the NIPP across the 18 critical

[22] GAO/AIMD-00-21.3.1.

[23] See generally Pub. L. No. 107-296, tit. II, 116 Stat. 1235, 2145 (2002), as amended.

[24] The Office of Infrastructure Protection generally relies on voluntary efforts to secure critical infrastructure because of its limited authority to directly regulate most critical infrastructure; however, other entities may possess and exercise regulatory authority over critical infrastructure to address security, such as for the chemical, transportation, and nuclear sectors. Our past work has shown that DHS leverages existing regulatory frameworks, where applicable, to implement the NIPP with its security partners within and across the 18 sectors and identify critical infrastructure security overlaps and gaps to enhance and supplement existing sector regulations. See GAO-11-537R.

infrastructure sectors; overseeing the development of Sector-Specific Plans; providing training and planning guidance to SSAs and asset owners and operators on protective measures to assist in enhancing the security of infrastructure within their control; and helping state, local, tribal, territorial, and private sector partners develop the capabilities to mitigate vulnerabilities and identifiable risks to their assets.

Within the Office of Infrastructure Protection, IASD manages the NCIPP. According to DHS, the main goals of the NCIPP are to (1) identify the infrastructure that if disrupted or destroyed could significantly affect the nation’s public health and safety, economic, or national security; (2) increase the accuracy of infrastructure prioritization efforts used to inform DHS resource allocation decisions; and (3) focus planning, foster coordination, and support preparedness efforts for incident management, response, and restoration activities among federal, state, and private sector partners. Critical infrastructure identified through the program includes several thousand level 1 or level 2 assets and systems. The levels are used to enhance decision making related to infrastructure protection and can include a range of businesses or assets in a local geographic area, such as refineries, water treatment plants, or commercial facilities, as well as the information and data systems that ensure their continued operation.

Consistent with the generally voluntary critical infrastructure protection approach identified in the NIPP, according to DHS, the success of the NCIPP relies upon the voluntary contributions and cooperation of public and private sector partners from the infrastructure protection community. To compile the NCIPP list, consistent with statutory requirements, IASD conducts a voluntary annual data call to solicit nominations to the list from state homeland security and federal partners. To submit nominations, partners are to develop realistic scenarios for infrastructure that meet specific criteria developed by IASD. Consistent with the consequence categories identified in the NIPP risk management framework, NCIPP nominations are to meet minimum specified consequence thresholds outlined in the annual data call for at least two of the following four categories: fatalities, economic loss, mass evacuation length, and degradation of national security.[25] After nominations are submitted, according to DHS guidance, IASD conducts a multiphase adjudication process intended to give state and federal partners the opportunity to review IASD's preliminary decisions and submit additional information to support nominations that were not initially accepted, before IASD finalizes the NCIPP list.[26]

Uses of the NCIPP List

The NCIPP list is used to establish risk management priorities. According to the NIPP, prioritizing risk management efforts provides the basis for understanding potential risk mitigation benefits that are used to inform planning and resource decisions.[27] The NCIPP list, which identifies nationally significant critical infrastructure based on consequences, informs the NIPP risk management prioritization process. The NIPP risk management prioritization process involves analyzing risk assessment results to determine which critical infrastructure faces the highest risk so that management priorities can be established. The NCIPP list is also used to, among other things:

[25] The precise consequence thresholds for inclusion on the NCIPP list are information that DHS designated "for official use only." We have not included this information in this report so that we could publicly present the results of our work. The four consequence categories identified in the NIPP include public health and safety (fatalities, injuries/illness), economic (direct and indirect costs), psychological (effect on public morale and confidence in national economic and political institutions), and governance/mission impact (effect on government's or industry's ability to maintain order, deliver minimal essential public services, etc.).

[26] IASD accepts nominations from three SSAs using an alternative adjudication process. Specifically, IASD accepts nominations from the Department of Defense—the defense industrial base SSA—directly to the NCIPP list because they only need to meet the national security criteria. IASD also accepts nominations made by the U.S. Coast Guard directly to the NCIPP list based on the sophistication of the Maritime Security Risk Analysis Model it uses to identify critical infrastructure meeting the NCIPP criteria. Additionally, IASD officials told us that they estimate evacuation impacts to supplement fatality estimates submitted under the Chemical Facility Anti-Terrorism Standards to determine which chemical facilities to add to the NCIPP list.

[27] Broadly defined, risk management is a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty. The NIPP risk management framework calls for critical infrastructure partners to assess risk from any scenario as a function of consequence, vulnerability, and threat. For the purposes of the NIPP, consequence—the effect of an event—is divided into four categories: public health and safety, economic, psychological, and governance/mission impact. The NIPP identifies vulnerability as the likelihood that an attack is successful, given that it is attempted, and threat is generally estimated as the likelihood of an attack being attempted by an adversary.

- Allocate Homeland Security Grants. Within DHS, FEMA uses the number of assets included on the NCIPP list, among other data, in its risk formula for allocating State Homeland Security Program (SHSP) and UASI grant funds. The SHSP and UASI provide funding to states and cities, respectively, to support a range of preparedness activities to prevent, protect against, respond to, and recover from acts of terrorism and other catastrophic events.[28] While the number of critical infrastructure a state or city has on the NCIPP list is used to determine the allocation of SHSP and UASI grant funds, there is no requirement that states or cities use these grant funds to enhance protection of these assets. For fiscal year 2012, FEMA allocated $294 million in SHSP funding to all 50 states, the District of Columbia, Puerto Rico, American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands. Additionally, in fiscal year 2012, FEMA allocated approximately $490 million in UASI funding to the nation's 31 highest-risk cities.

- Prioritize Voluntary Critical Infrastructure Protection Programs. The Office of Infrastructure Protection's Protective Security Coordination Division (PSCD) uses the NCIPP list and other inputs to prioritize its efforts to work with critical infrastructure owners and operators and state and local responders to (1) assess vulnerabilities, interdependencies, capabilities, and incident consequences, and (2) develop, implement, and provide national coordination for protective programs. Related to these efforts, PSCD has deployed the aforementioned PSAs in 50 states and Puerto Rico to locations based on population density and major concentrations of critical infrastructure. PSAs use the NCIPP list to prioritize outreach to level 1 and level 2 assets in their area of jurisdiction for participation in DHS's voluntary security survey and vulnerability assessment programs, such as the Enhanced Critical Infrastructure Protection and Site

[28] See GAO, *DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs,* GAO-12-303 (Washington, D.C.: Feb. 28, 2012). Additionally, FEMA allocates UASI funds to high-threat, high-density urban areas referred to as metropolitan statistical areas (MSA). For ease of reporting, we will refer to UASI grant recipients as cities rather than MSAs.

Assistance Visit programs.[29] PSAs are also often called upon by state homeland security advisers to assist them in nominating assets to the NCIPP list.

- Inform Incident Management Planning and Response Efforts. DHS uses information collected during the NCIPP process and the NCIPP list to inform and prioritize incident management planning and response efforts. When an incident occurs, DHS officials pull information from a variety of sources, including the database of assets nominated to and accepted on the NCIPP list, to identify critical infrastructure in the affected area. IASD then prioritizes this information in an infrastructure of concern list to guide incident response efforts. The infrastructure of concern list includes any critical infrastructure affected by the event, which may include level 1 or level 2 assets.[30] IASD provides the infrastructure of concern list to other DHS components, including FEMA and PSAs, who use it on the ground to guide local incident response efforts.

DHS Has Made Changes to NCIPP List Criteria, but Has Not Identified the Impact of These Changes or Validated Its Approach

DHS has made several changes to its criteria for including assets on the NCIPP list. These changes initially focused on introducing criteria to make the lists entirely consequence based, with subsequent changes intended to introduce specialized criteria for some sectors and assets. DHS's changes to the NCIPP criteria have changed the composition of the NCIPP list, which has had an impact on users of the list. However, DHS does not have a process to identify the impact of these changes on users nor has it validated its approach for developing the list.

[29] Enhanced Critical Infrastructure Protection security surveys are voluntary half- to full-day surveys DHS conducts to assess asset security and increase security awareness, the results of which are presented to critical infrastructure owners and operators in a way that allows them to see how their assets' security measures compare with those of similar assets in the same sector. Site Assistance Visits are voluntary vulnerability assessments that can take up to 3 days to complete and identify security gaps at assets. Results from these assessments are used to provide options to enhance security measures and resilience to critical infrastructure owners and operators.

[30] According to DHS officials, level 1 or level 2 assets are included on an infrastructure of concern list only if the specific event is expected to or does affect those assets in a way that would cause significant effects. Any level 1 or level 2 assets on the infrastructure of concern list are not identified as such because the NCIPP list is classified.

DHS Made Several Changes to the List Criteria and Format

DHS's initial approach for developing the NCIPP list differed by asset level. According to the Homeland Security Act, as amended, DHS is required to establish and maintain a prioritized list of systems and assets that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects.[31] The criteria for level 1 assets focused on consequences—the effects of an adverse event. The criteria for level 2 assets focused generally on capacity—the number of people that use an asset or output generated by an asset, such as the number of people that occupy a commercial office building, the daily ridership of a mass transit system, or the number of people served by a water utility. DHS officials told us that the level 1 consequence-based criteria and thresholds were initially established at the beginning of the program at the discretion of the Assistant Secretary for Infrastructure Protection, who sought to identify infrastructure that the destruction of which could be expected to cause impacts similar to those caused by the attacks of September 11 and Hurricane Katrina.[32] In contrast, the initial level 2 criteria were generally capacity based in order to identify the most critical assets within each of the 18 sectors. However, the capacity-based criteria often differed by sector, making it difficult to compare criticality across sectors and therefore identify the highest-priority critical infrastructure on a national level.

DHS Revised List Criteria in 2009 to Be Entirely Consequence Based

In 2009, DHS changed the level 2 criteria to make the NCIPP list entirely consequence based, a change that brought its approach more into line with statutory requirements and, consistent with the NIPP risk management framework, allowed for comparison across sectors. The new level 2 criteria match the level 1 consequence-based criteria—fatalities, economic loss, mass evacuation length, or national security impacts—but with lower threshold levels than those used to identify level 1 assets.[33] To be included on the NCIPP list, an asset must meet at least

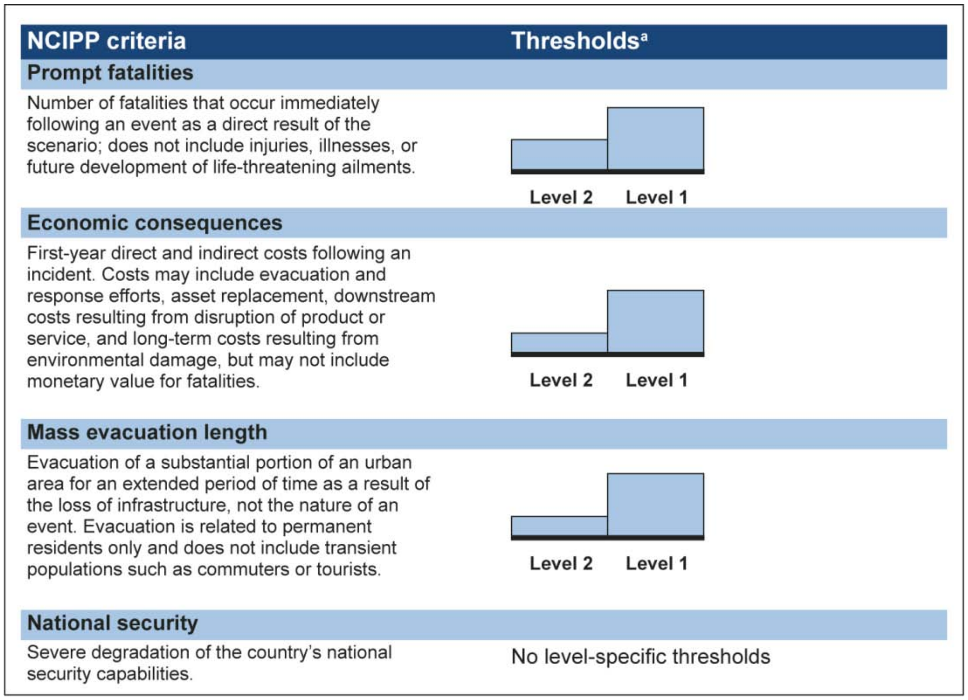
[31] See 6 U.S.C. § 124*l*(a)(2). According to DHS officials, the Secretary of Homeland Security delegated responsibility for developing the NCIPP list to the Assistant Secretary for Infrastructure Protection.

[32] DHS could not provide documentation explaining how the threshold levels were established because, according to officials, the agency undertook an information technology change in the spring of 2012 that resulted in the loss of agency e-mails and program documentation. Further, officials noted the loss of institutional knowledge because of staff changes.

[33] DHS officials told us that the level 2 consequence-based thresholds were developed using the level 1 consequence-based thresholds, then lowered based on internal agency discussions and dialogue with subject matter experts.

two of the four consequence thresholds, and is included on the list as either level 1 or level 2 depending on which consequence thresholds it meets. As figure 1 shows, the level 1 thresholds are higher than level 2 thresholds and therefore represent the most nationally critical assets.

Figure 1: National Critical Infrastructure Prioritization Program (NCIPP) Consequence-Based Criteria and Relative Threshold Levels



NCIPP criteria	Thresholds[a]
Prompt fatalities	
Number of fatalities that occur immediately following an event as a direct result of the scenario; does not include injuries, illnesses, or future development of life-threatening ailments.	Level 2 Level 1
Economic consequences	
First-year direct and indirect costs following an incident. Costs may include evacuation and response efforts, asset replacement, downstream costs resulting from disruption of product or service, and long-term costs resulting from environmental damage, but may not include monetary value for fatalities.	Level 2 Level 1
Mass evacuation length	
Evacuation of a substantial portion of an urban area for an extended period of time as a result of the loss of infrastructure, not the nature of an event. Evacuation is related to permanent residents only and does not include transient populations such as commuters or tourists.	Level 2 Level 1
National security	
Severe degradation of the country's national security capabilities.	No level-specific thresholds

Source: GAO analysis of DHS documents.

[a] A scale for this graphic is not provided because the exact threshold levels for the NCIPP criteria are designated "for official use only." We have not included this information in this report so that we could publically present the results of our work.

According to officials and agency documents, DHS changed the level 2 criteria to be consequence based for several reasons. First, NCIPP program officials stated that they changed the criteria to align the list with statutory requirements. Specifically, DHS interpreted the statute's requirement that it identify assets that "would, if destroyed or disrupted, cause national or regional catastrophic effects," as a call for consequence-based criteria.[34] Program officials told us that their analysis of assets prioritized using capacity-based criteria demonstrated that the initial level 2 criteria were not sufficient to fully identify assets capable of causing catastrophic events. Second, program officials stated that they changed the criteria to allow for comparisons across sectors, which is consistent with the NIPP. The NIPP states that using a common approach with consistent assumptions and metrics increases the ability to make comparisons across sectors, different geographic regions, or different types of events. Third, DHS also changed the criteria to improve the utility of the list. According to the NCIPP guidance, prior to 2009, assets designated as level 2 on the list experienced instability—assets being added and removed from year to year—which frustrated efforts to use the list for risk management planning and engagement, while assets designated as level 1 on the list—which had always been consequence based—remained relatively stable year to year.

DHS Made Additional Changes to Criteria for Some Sectors and High-Risk Assets

Since 2009, DHS has continued to make changes to the NCIPP criteria by creating specialized criteria for some sectors and assets. In 2010, DHS introduced specialized criteria for the agriculture and food sector. According to NCIPP program officials, the newly established level 2 consequence-based criteria did not account for the unique criticality of the agriculture and food sector, which is characterized by a high degree of connectivity because of the movement of animals and other food products. Specifically, they explained that the established consequence criteria were unable to account for the fact that individual animals could be the entry point for a scenario—such as malicious contamination with an agent like foot-and-mouth disease—which may cause catastrophic effects.[35] The introduction of the agriculture and food sector-specific criteria resulted in more than double the number of assets included on the fiscal year 2011 NCIPP list for that sector over the previous list. However,

[34] See 6 U.S.C. § 124*l*(a)(2).

[35] Foot-and-mouth disease (FMD) is a highly contagious viral disease of cloven-hoofed animals such as cattle, swine, and sheep. Infected animals develop a fever and blisters on their tongue and lips, and between their hooves. Many animals recover from a FMD infection, but the disease leaves them debilitated and causes losses in meat and milk production. FMD does not have human health implications. According to the U.S. Department of Agriculture, a 2001 outbreak of FMD in the United Kingdom resulted in the slaughter of millions of animals and economic losses conservatively estimated at $14.7 billion. See GAO, *Homeland Security: Actions Needed to Improve Response to Potential Terrorist Attacks and Natural Disasters Affecting Food and Agriculture*, GAO-11-652 (Washington D.C.: Aug. 19, 2011).

DHS is currently reevaluating the agriculture and food sector-specific criteria because, according to officials, the specialized criteria created a great deal of inconsistency in the agriculture and food assets and systems included on the NCIPP list year to year.

In 2010, DHS also made adjustments to the NCIPP criteria to account for high-risk assets that may not always meet the consequence criteria by introducing the Catastrophic Economic Impacts Project and the Threats to Infrastructure Initiative. Under the Catastrophic Economic Impacts Project, infrastructure that meets only the level 1 consequence threshold for economic impact, but no other criteria, is added to the list as a level 2 asset. DHS officials explained that the project was added to account for instances when economic impact may be the primary impact. For example, the officials noted that a collapse of the U.S. financial system would likely not cause a large number of prompt fatalities or evacuations, but would cause catastrophic national impacts nonetheless. Meanwhile, the Threats to Infrastructure Initiative allows infrastructure that has received a specific, credible threat from a malicious actor, but otherwise would not meet NCIPP list criteria, to be added to the list as a level 2 asset. Unlike the other NCIPP criteria, the Threats to Infrastructure Initiative focuses on the threat to infrastructure rather than the consequences that may result from a specific event, which could complicate comparisons across assets and sectors. DHS officials told us that infrastructure with specific and credible threats were always included on the NCIPP list, but were historically added based on information from the intelligence community.[36] The addition of the initiative allowed states to nominate critical infrastructure under the same scenario based on state and local intelligence information, such as that collected by fusion centers.[37] According to DHS officials, they adjudicate Threats to Infrastructure Initiative nominations by determining whether the threat to

[36] See 50 U.S.C. § 401a(4) (listing the 17 elements that compose the U.S. intelligence community).

[37] See 6 U.S.C. § 124h(j)(1) (defining "fusion center" as a collaborative effort 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 detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity). As of February 2013, there were 78 fusion centers nationwide.

an asset is specific and credible.[38] As of fiscal year 2012, approximately 60 assets and systems have been added to the NCIPP list as a result of these new criteria.[39]

DHS Changed the List Format to Include Clusters and Systems of Infrastructure

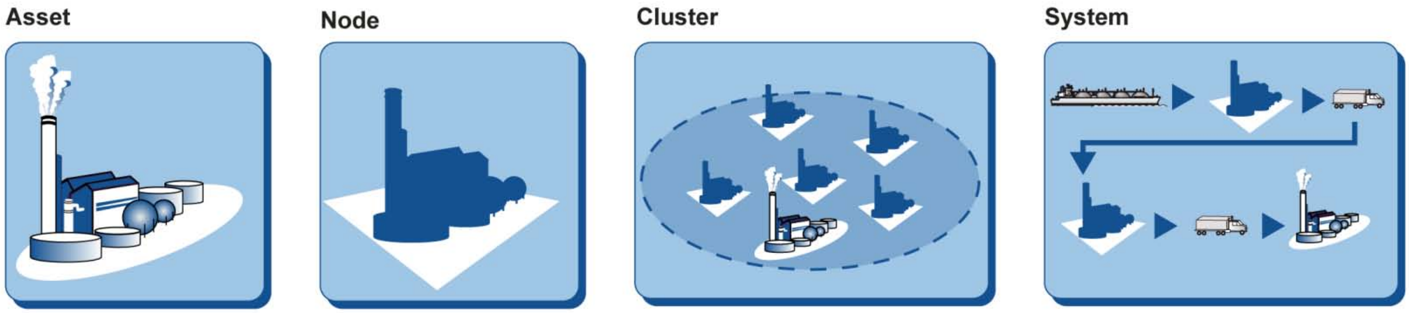
In 2009, DHS also changed the format of the NCIPP list by expanding the type of infrastructure that could be nominated to the list to include clusters and systems of critical infrastructure in an effort to characterize the relationship among some infrastructure, such as dependencies and interdependencies, which was consistent with the statute and NIPP.[40] According to the NCIPP guidance, clusters or systems of critical infrastructure are made up of two or more associated or interconnected assets or nodes that can be disrupted through a single event, resulting in regional or national consequences that meet the NCIPP criteria thresholds. An asset is a single facility with a fixed location that functions as a single entity (although it can contain multiple buildings or structures) and meets the NCIPP criteria by itself. A node is a single facility, similar to an asset, that does not meet the NCIPP criteria individually but does meet the criteria when grouped with other nodes or assets in a cluster or system. Figure 2 provides an illustration of an asset, a node, a cluster, and a system.

[38] According to NCIPP guidance, DHS considers a specific, credible threat to exist if an individual or group has demonstrated an intention to attack specific infrastructure and possesses the capability to execute an attack that, if successful, would significantly disrupt or destroy the infrastructure or cause loss of life.

[39] The precise number of assets on the NCIPP list is information that DHS designated “for official use only.” We have not included this information in this report so that we could publically present the results of our work.

[40] According to DHS documents, examples of infrastructure interdependencies include colocation, geographic proximity, and common cyber vulnerabilities.

Figure 2: Description and Illustration of an Asset, a Node, a Cluster, and a System



Asset

An asset is a single facility with a fixed location that functions as a single entity.

Assets are nominated to the NCIPP list for meeting the criteria by themselves.

Node

A node is a single facility, similar to an asset, but does not meet the NCIPP list criteria by itself.

Nodes are not nominated for individual consideration for inclusion on the list.

Cluster

A cluster is a group of two or more associated infrastructure facilities (assets or nodes) that can be disrupted through a single natural or man-made event, resulting in regional or national consequences.

Clusters are nominated for inclusion on the NCIPP list.

System

A system is a group of two or more interconnected infrastructure facilities (assets or nodes) that can be disrupted through a single natural or man-made event, resulting in regional or national consequences.

Systems are nominated for inclusion on the NCIPP list.

Source: GAO analysis of DHS documents.

Because nodes do not meet the NCIPP criteria on their own, they are not included on the NCIPP list, but are identified on a separate list that is associated with the NCIPP list. For example, a group of nodes or assets making up a cluster would be listed on the NCIPP list under the name of the cluster, such as the ABC Cluster, but one would have to consult the associated list of nodes to identify the specific facilities that make up the listed cluster.[41] The concept of clusters and systems is consistent with the statute and NIPP risk management framework. The law states that the prioritized list of critical infrastructure shall contain both systems and assets included in the national asset database, and the NIPP states that to the extent possible, risk assessments should assess the dependencies and interdependencies associated with each identified asset, system, or network. According to DHS, they recognized a need to identify clusters of critical infrastructure in 2008 after Hurricanes Gustav and Ike damaged a group of refineries that resulted in a nationally significant supply disruption of certain petrochemicals used across a wide range of industries.

[41] The example provided is intended to illustrate the concept of a cluster.

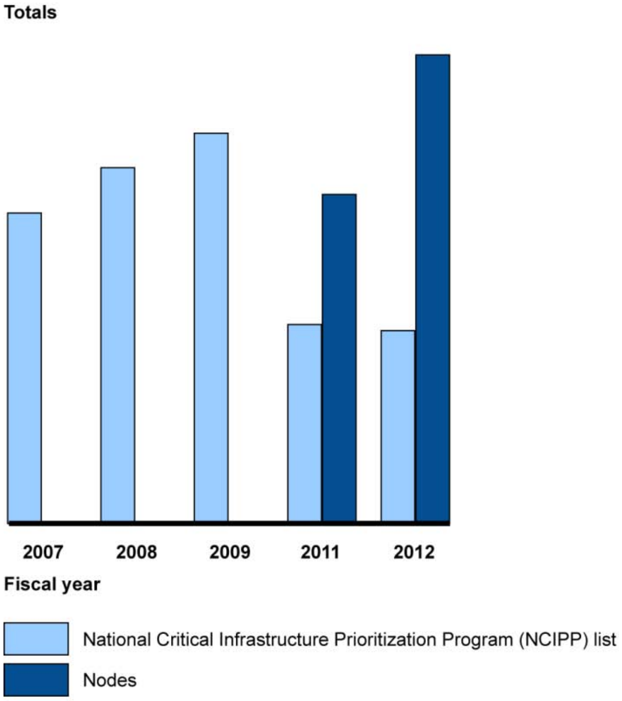
DHS Has Not Identified the Impact of Changes in Criteria on List Users or Validated Its Approach for Developing the List

The changes DHS made to the NCIPP criteria in 2009 and 2010 changed the number of assets on and the composition of the NCIPP list. The total number of assets, clusters, and systems on the NCIPP list decreased from more than 3,000 in fiscal year 2009 to fewer than 2,000 in fiscal year 2011.[42] The introduction of clusters and systems resulted in a separate list of thousands of nodes associated with the NCIPP list. Specifically, more than 2,500 additional facilities were included on the first nodes list in fiscal year 2011, and almost 4,000 facilities were included on the nodes list for fiscal year 2012.[43] Figure 3 shows the relative changes in the number of assets, clusters, and systems on the NCIPP list and associated nodes list for fiscal years 2007 through 2012.

[42] Because of the challenges encountered with changes DHS made to the NCIPP criteria in 2009, the fiscal year 2010 NCIPP list was not approved by the Assistant Secretary for Infrastructure Protection and therefore not finalized or used. Additionally, the precise number of assets on the NCIPP list is information that DHS designated “for official use only.” We have not included this information in this report so that we could publically present the results of our work.

[43] According to DHS officials, a node may be included in more than one cluster or system. In this case, the node would be listed on the nodes list multiple times.

Figure 3: Relative Changes in the Total Number of Assets on the National Critical Infrastructure Prioritization Program List and Associated Nodes List, Fiscal Years 2007-2009 and 2011-2012

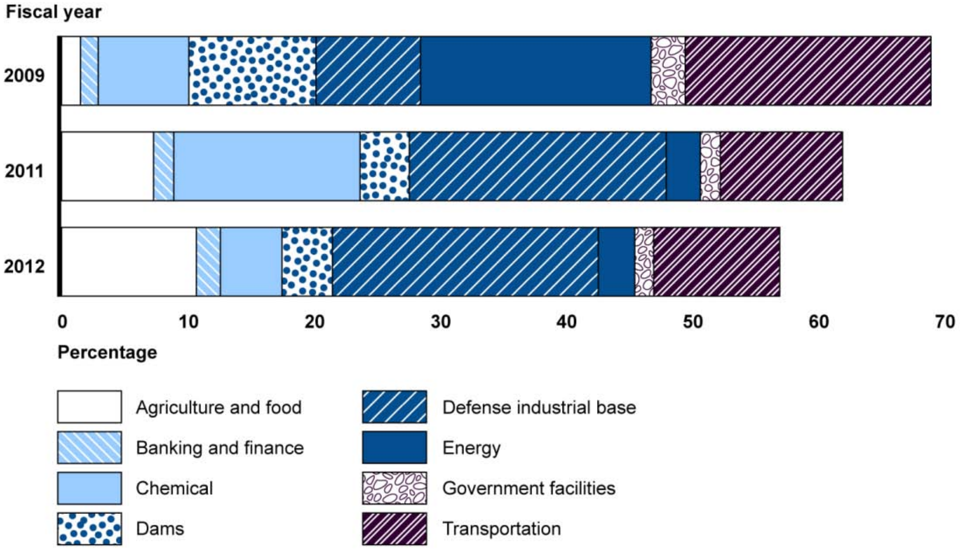


Source: GAO analysis of DHS data.

Note: A scale for this graphic is not provided because the total number of NCIPP listed assets and associated nodes are designated "for official use only." We have not included this information in this report so that we could publically present the results of our work. Additionally, because of the challenges encountered with changes DHS made to the NCIPP criteria in 2009, the fiscal year 2010 NCIPP list was not approved by the Assistant Secretary for Infrastructure Protection and therefore not finalized or used.

Additionally, the criteria changes also resulted in a change in the distribution of assets, clusters, or systems included on the NCIPP list by sector. Figure 4 shows that, among other sectors, the distribution of assets in the agriculture and food and defense industrial base sectors experienced large increases as a percentage distribution of the list from fiscal years 2009 to 2011, while for the same period, the energy and transportation sectors experienced large decreases. It also shows that the distribution of assets in the agriculture and food sector continued to increase as a percentage distribution of the list from fiscal years 2011 to 2012, while for the same period, the chemical sector experienced a large decrease.

Figure 4: Distribution of Critical Assets on the National Critical Infrastructure Prioritization Program List by Select Sectors, Fiscal Year 2009 (before Change to Consequence-Based Criteria) and Fiscal Years 2011 and 2012 (after Change to Consequence-Based Criteria)



Source: GAO analysis of DHS data.

Note: The sectors presented above reflect the 8 sectors we selected to focus on for this report. For more information on how we selected these sectors, see appendix II. The remaining portion of the list not presented above includes assets in the remaining 10 sectors including the health care and public health; national monuments and icons; water; commercial facilities; critical manufacturing; emergency services; nuclear reactors, materials and waste; information technology; communications; and postal and shipping sectors. Additionally, because of the challenges encountered with changes DHS made to the NCIPP criteria in 2009, the fiscal year 2010 NCIPP list was not approved by the Assistant Secretary for Infrastructure Protection and therefore not finalized or used.

Changes in the List Can Have an Impact on List Users, but DHS Does Not Have a Process for Identifying the Impact of These Changes

Our analysis shows that changes to the NCIPP list can have an impact on users of the list, specifically, FEMA's allocation of UASI grant funds and PSAs' ability to prioritize outreach and conduct site visits for its protection programs. Our analysis of the FEMA risk formula shows that a change in the number of NCIPP-listed assets located in a city has an impact on a city's relative risk score. Our analysis also shows that current UASI grant allocations are strongly associated with a city's current relative risk score.[44] Therefore, a change in the number of NCIPP-listed assets located in a city can have an impact on the level of grant funding it

[44] This is the case even when accounting for the strong association between current grant allocations and the previous year's grant allocation.

receives.[45] For example, in fiscal year 2012, FEMA allocated approximately $490 million in UASI grant funds to the 31 cities with the highest relative risk scores out of 102 eligible cities nationwide. Our analysis of FEMA's risk formula showed that, at the minimum, if the number of level 2 assets is increased or decreased by as few as two for each city, it would change the relative risk score for 5 of the 31 cities that received fiscal year 2012 UASI grant funding. Such a change could result in increased or decreased grant funding allocations for the affected cities. The changes in the relative risk scores tend to affect cities in the middle to the bottom of the top 31 list because there is generally a larger gap between the relative risk scores of those cities at the top of the list than those in the middle to bottom of the list. However, even a small change in grant funding could have an impact on a city, especially if that city does not traditionally receive other federal assistance as compared with cities with higher risk scores.

We previously reported that changes to the NCIPP list have presented challenges to managing DHS programs, particularly the voluntary security survey and assessment programs managed by PSCD. In May 2012, we reported that PSCD was unable to track the extent to which it conducted security surveys and vulnerability assessments on NCIPP level 1 and level 2 assets because of (1) inconsistencies between the databases used to identify the high-priority assets and to identify surveys and assessments completed, and (2) the change in the format and organization of the NCIPP list that converted some assets previously listed as level 1 or level 2 into a cluster or system.[46] Beginning with the fiscal year 2012 NCIPP list, DHS has begun to assign unique numerical identifiers to each NCIPP asset, cluster, and system, which officials told us has helped DHS track how many security surveys and vulnerability assessments it conducts on high-priority assets. The officials also told us that they anticipate fewer challenges associated with the list since the

[45] The FEMA risk formula also values level 1 assets more than level 2 assets. Thus, changes in the number of assets a city has at each level—either a level 1 asset being transferred to the level 2 list or multiple level 2 assets being consolidated into a cluster—could also have an impact on its relative risk score and therefore its grant funding allocation.

[46] According to DHS officials, adding clusters to the list also resulted in multiple entries on the list, such as a duplicate entry for an asset that spans two states, multiple entries for a single asset that is listed both individually and in relation to a cluster or system, and multiple entries for a single asset within several clusters or systems. See GAO-12-378 for details.

number of assets, clusters, and systems on the NCIPP list has remained relatively stable from fiscal years 2011 to 2012. However, as discussed earlier, the number of nodes associated with the NCIPP list has increased substantially, growing from more than 2,500 in fiscal year 2011 to almost 4,000 in fiscal year 2012, which could further challenge PSA's ability to conduct outreach and prioritize site visits to critical infrastructure for its protection programs.

PSCD officials in Washington, D.C. further told us that they do not have criteria establishing how PSAs should assess an NCIPP cluster or system that may contain many different nodes. The number of nodes in an NCIPP cluster or system can vary from two to several dozen and may be geographically dispersed. For example, one PSA told us that nodes in the same cluster may not have the same owner and could be part of a multistate system. Another PSA said that because several nodes in a system may not be the same (i.e., different types of facilities, different facility owners, or located in different areas), he generally conducts an assessment of each node in order to consider an assessment of a system complete. He explained that the facilities would have to be identical in order to conduct a single assessment for separate nodes, which he noted is rarely the case. Because it is difficult to prioritize which nodes within clusters or systems may be the most important for conducting assessments, the increase in the number of nodes associated with the NCIPP list could have the effect of complicating PSA efforts to conduct outreach to and assessments on the nation's highest-priority infrastructure. PSCD officials told us they view this as a challenge, but they do not characterize it as a significant challenge. Further, they stated that while the treatment of nodes within NCIPP clusters or systems has not been specifically addressed in current program policies or guidance, they do not believe that this challenge has affected their ability to effectively prioritize facilities to receive security surveys and assessments. In January 2013, a PSCD official told us that PSCD is considering new guidance that would clarify how PSAs should approach nodes when conducting outreach or prioritizing visits for voluntary protection programs.

DHS does not have a process for identifying the impact of changes to the list on its users and has not reviewed the impact of these changes on users. However, program officials told us that they work closely with the primary users of the list to understand how the data are used. According to officials, they recognize that changes to the NCIPP list may have an impact on users of the list, but they consider these impacts to be minor. For example, one program official told us that the changes in the number of level 1 and level 2 assets rarely have a significant effect on the amount of grant funding allocated to states or cities, because of the additional inputs considered in the FEMA risk formula that determine the grant allocations. However, as previously demonstrated through our analysis, even small changes to the NCIPP list counts can have an impact on UASI grant allocations when accounting for all of the additional inputs considered in FEMA's risk formula. The officials also recognized that changes from the fiscal year 2009 to fiscal year 2011 NCIPP lists, which significantly reduced the number of assets on the list, required PSCD to reset its performance metrics for conducting its voluntary security survey and assessment programs.[47] However, officials told us that the assets on the NCIPP list have remained relatively stable since fiscal year 2011; therefore, the officials believe that changes to the list would have a minor impact on PSAs' outreach activities. While our analysis shows that the number of assets on the NCIPP list remained fairly constant from fiscal year 2011 to 2012, it also shows that the number of nodes on the associated nodes list continued to grow and almost doubled during this time. As discussed, the increase in nodes may complicate PSA efforts to conduct outreach to and assessments on the nation's highest-priority infrastructure. Additionally, the officials told us that, internally, changes to the NCIPP list do not have an impact on DHS's ability to identify and prioritize critical infrastructure during an incident because the list is just one of many information sources they consult when developing an event-specific infrastructure of concern list to guide incident response efforts.

DHS Has Not Validated NCIPP Criteria and Approach to Ensure That the List Identifies the Highest-Priority Critical Infrastructure

While the change to an entirely consequence-based list created a common approach to identify infrastructure and align the program with the statute and NIPP, recent and planned criteria changes to accommodate certain sectors and assets represent a departure from this common approach, which could hinder DHS's ability to compare infrastructure across sectors. For example, the agriculture and food sector has criteria that are different from those of all other sectors. Furthermore, DHS has not validated its approach to developing the list to ensure that it accurately reflects the nation's highest-priority critical infrastructure.

[47] We previously reported that PSCD's Deputy Director told us that PSCD had a goal that 50 percent of the security surveys and vulnerability assessments conducted each year be on level 1 or level 2 assets. However, this goal was not documented, and we recommended that PSCD institutionalize realistic performance goals for appropriate levels of participation in security surveys and vulnerability assessments by high-priority assets to measure how well DHS is achieving its goals. See GAO-12-378 for details.

The NIPP calls for risk assessments—such as NCIPP efforts—to be complete, reproducible, documented, and defensible to produce results that can contribute to cross-sector risk comparisons for supporting investment, planning, and resource prioritization decisions.[48] Table 1 provides a description of these core criteria for risk assessments.

Table 1: *National Infrastructure Protection Plan* (NIPP) Core Criteria for Risk Assessments

Criterion	Description
Complete	The methodology should assess consequence, vulnerability, and threat for every defined risk scenario and follow the more specific guidance given in NIPP, such as documenting the scenarios assessed, estimating the number of fatalities, describing all protective measures in place, and identifying attack methods that may be employed.[a]
Reproducible	The methodology must produce comparable, repeatable results, even though assessments of different critical infrastructure and key resources may be performed by different analysts or teams of analysts. It must minimize the number and impact of subjective judgments, leaving policy and value judgments to be applied by decision makers.
Documented	The methodology and the assessment must clearly document what information is used and how it is synthesized to generate a risk estimate. Any assumptions, weighting factors, and subjective judgments need to be transparent to the user of the methodology, its audience, and others who are expected to use the results. The types of decisions that the risk assessment is designed to support and the timeframe of the assessment (e.g., current conditions versus future operations) should be given.
Defensible	The risk methodology must logically integrate its components, making appropriate use of the professional disciplines relevant to the analysis, and be free from significant errors or omissions. Uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates should be communicated.

Source: 2009 NIPP.

[a] During the National Critical Infrastructure Prioritization Program (NCIPP) adjudication phase, DHS assesses the threat and vulnerability of each NCIPP nomination based on the disruption scenario submitted to determine if the scenario could realistically be expected to produce impacts meeting the NCIPP consequence criteria and threshold levels.

DHS could not provide documentation explaining how the threshold levels were established, such as the methodology for developing the NCIPP criteria or the analysis used to support the criteria, because, according to agency officials, the agency undertook an information technology change in the spring of 2012 that resulted in the loss of agency e-mails and program documentation. Nevertheless, as previously noted, officials told us the criteria and thresholds were established at the discretion of the Assistant Secretary for Infrastructure Protection. Program officials noted that they review the list on an annual basis but that the list has not been independently verified and validated by an external peer review. These officials believe a peer review would enable DHS to determine whether its

[48] DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency*.

efforts to develop the NCIPP list are based on analytically sound methodology and whether it has appropriate procedures in place to ensure that the NCIPP list is defensible and reproducible.

We have previously reported that peer reviews are a best practice in risk management[49] and that independent expert review panels can provide objective reviews of complex issues.[50] An independent peer review to validate the NCIPP criteria and list development process would better position DHS to reasonably assure that, consistent with the NIPP risk management framework, federal and state partners that use the NCIPP list have sound information when making risk management and resource allocation decisions. According to the NIPP, having sound information for making those decisions is critical for focusing attention on those protection and resiliency activities that bring the greatest return on investment.

In August 2012, NCIPP program officials told us they would like to establish a peer review to validate the program because officials believe the list has stabilized and now consider the program to be in a “maintenance phase.” In December 2012, the program director told us that IASD drafted and submitted a proposal to the Assistant Secretary for Infrastructure Protection in November 2012 that proposed different approaches for reviewing the NCIPP, including a peer review of the criteria used to decide which assets and systems should be placed on the list and the process for doing so. At that time, DHS officials said that they could not provide a copy of the draft proposal because it had not been approved by management. As of January 2013, IASD told us that the proposal had not been submitted to the Assistant Secretary for Infrastructure Protection as originally discussed, that it was unclear when the proposal would be submitted, and that it remained uncertain whether a peer review would be approved.

[49] Peer review is the process of subjecting scholarly work, research, or ideas to the scrutiny of others who are experts in the same field. Such review is considered a form of scientific validation. See GAO, *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*, GAO-12-14 (Washington, D.C.: Nov. 17, 2011).

[50] See GAO, *Aviation Security: Efforts to Validate TSA’s Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*, GAO-10-763 (Washington, D.C.: May 20, 2010).

The National Research Council of the National Academies has also recommended that DHS improve its risk analyses for infrastructure protection by validating the models and submitting them to external peer review.[51] According to the council, periodic reviews and evaluations of risk model outputs are important for transparency with respect to decision makers.[52] These reviews should involve specialists in modeling and in the problems that are being addressed and should address the structure of the model, the types and certainty of the data, and how the model is intended to be used. Peer reviews can also identify areas for improvement. As we have previously reported, independent peer reviews cannot ensure the success of a model, but they can increase the probability of success by improving the technical quality of projects and the credibility of the decision-making process.[53] Thus, an independent peer review would better position DHS to provide reasonable assurance that the NCIPP criteria and list development process is reproducible and defensible given the recent and planned changes, and that critical infrastructure protection efforts are being prioritized on the nation's highest-priority infrastructure as intended by the NIPP risk management framework.

DHS Has Taken Actions to Improve Its Consultation with States and SSAs to Address Challenges Developing the NCIPP List

DHS has taken various actions to work with states and SSAs, consistent with statutory requirements and the NIPP, to identify and prioritize critical infrastructure. However, officials representing selected states and SSAs have mixed views about their experiences adjusting to DHS's changes to the NCIPP. DHS recognizes that states, in particular, face challenges—such as resource and budgetary constraints—associated with nominating assets to the NCIPP list, and has taken actions to address these challenges and reduce the burden on states.

[51] National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, D.C.: 2010).

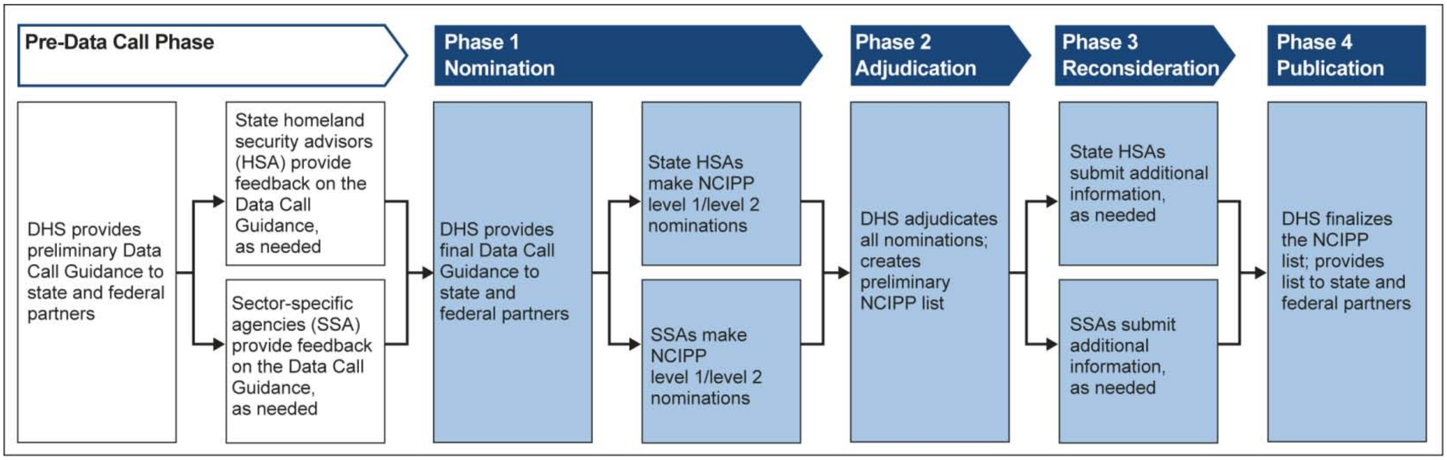
[52] See National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis*.

[53] See GAO-12-14 and GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington D.C.: Mar. 31, 2004).

DHS Has Taken Various Actions to Work with States and SSAs on Developing the List

In recent years, DHS has taken actions to improve its outreach to states and SSAs to obtain their input on changes to the NCIPP. In 2009, DHS's outreach to states and SSAs consisted of issuing a memorandum to obtain input on the proposed change to consequence-based criteria.[54] Since 2009, DHS has taken various actions to address state nomination challenges and to reduce the burden on states. For example, in 2009, DHS revised its list development process to be more transparent and provided states with additional resources and tools for developing their NCIPP nominations. Specifically, once states submit their NCIPP nominations, DHS is to make preliminary adjudication determinations based upon the NCIPP criteria, then provide its preliminary adjudication results (whether a nomination was accepted or not) and why the decision was made. Next, DHS is to allow states an opportunity to request reconsideration of the nomination for which they could provide additional documentation clarifying the eligibility of the infrastructure. Figure 5 shows the revised NCIPP list development process, including the nomination, adjudication, and reconsideration phases.

Figure 5: National Critical Infrastructure Prioritization Program (NCIPP) List Development Process



Pre-Data Call Phase

DHS provides preliminary Data Call Guidance to state and federal partners

State homeland security advisors (HSA) provide feedback on the Data Call Guidance, as needed

Sector-specific agencies (SSA) provide feedback on the Data Call Guidance, as needed

Phase 1 Nomination

DHS provides final Data Call Guidance to state and federal partners

State HSAs make NCIPP level 1/level 2 nominations

SSAs make NCIPP level 1/level 2 nominations

Phase 2 Adjudication

DHS adjudicates all nominations; creates preliminary NCIPP list

Phase 3 Reconsideration

State HSAs submit additional information, as needed

SSAs submit additional information, as needed

Phase 4 Publication

DHS finalizes the NCIPP list; provides list to state and federal partners

Source: GAO analysis of DHS documents.

[54] This action was consistent with provisions of the 9/11 Commission Act, which amended title II of the Homeland Security Act by requiring, among other things, that DHS regularly review its data collection guidelines and consult with appropriate state homeland security officials to solicit feedback about the guidelines, as appropriate, and the NIPP, which calls for DHS to work with critical infrastructure partners, including states and SSAs, to identify and prioritize the most critical assets, systems, and networks through the NCIPP list development process. See 6 U.S.C. § 124*l*(c)(1)(A), (B).

In addition to revising the adjudication process, DHS took several actions intended to improve the nomination process in recent years. First, according to DHS's 2011 data call guidance, DHS provided on-site assistance from subject matter experts to assist states with identifying infrastructure and disseminated a lessons learned document providing examples of successful nominations to help states improve justifications for nominations. Second, DHS has taken action to be more proactive in engaging states and SSAs in ongoing dialogue on proposed criteria changes and improving the NCIPP process and resulting list. For example, in 2010, DHS hosted the Food and Agriculture Criticality Working Group established through the Food and Agriculture Sector Government Coordinating Council—consisting of over 100 participants (including DHS, states, and SSAs)—to discuss the aforementioned modification of the criteria to make it more applicable to the agriculture and food sector. As discussed earlier, DHS and its state and SSA partners are currently reevaluating the agriculture and food sector-specific criteria, and the SSAs held a meeting in December 2012 to discuss updating and adding additional criteria. In addition, in July 2011, DHS established a working group composed of state and SSA officials to solicit feedback on the nomination process and recommend actions to improve the quality of the NCIPP list in preparation for the 2013 data call.[55] DHS officials told us that much of the feedback received from states and SSAs centered on DHS improving communication and guidance throughout the data call—for example, updating the guidance with additional information on criteria. DHS also planned long-term studies, such as requesting input from partners on modifying criteria thresholds. DHS officials told us that they conducted extensive outreach to states and SSAs to encourage participation in the NCIPP working group including extending the submission deadlines multiple times, funding an on-site meeting with the partners, and hosting webinars and conference calls. However, according to DHS officials, DHS has since disbanded the working group because of lack of state and SSA participation and DHS budget constraints.

[55] Although the 9/11 Commission Act provides that DHS shall regularly review the NCIPP guidelines and consult with appropriate homeland security officials of states, as appropriate, DHS is not specifically required to consult with SSAs. See 6 U.S.C. § 124*l*(c)(1)(B). Nevertheless, among the SSAs we interviewed, DHS consulted with five out of the eight SSAs prior to changing to consequence-based criteria in 2009. This is consistent with the NIPP partnership model, whereby DHS officials are to collaborate with senior-level partners, such as the sector coordinating councils, to coordinate a national framework for critical infrastructure protection and resilience within and across sectors.

Officials Representing Selected SSAs and States Have Mixed Views on the NCIPP Nomination Process

Despite DHS's outreach efforts, homeland security officials representing selected states and SSAs have mixed views on the NCIPP nomination process because of program changes, such as the aforementioned change to consequence-based criteria. Overall, the SSA officials we interviewed had more positive views of the NCIPP nomination process than the state officials we interviewed.

SSA officials representing five of the eight sectors we interviewed told us that they believe it is very easy or moderately easy to nominate assets to the NCIPP list.[56] However, officials representing three sectors said that they believe it is moderately difficult or very difficult to nominate assets to the list because of various factors. For example, one SSA official told us that the diversity and complexity of the sector's assets makes it difficult to determine which assets meet the NCIPP criteria. Also, one SSA official stated that the online tool that the SSA uses to nominate assets to the NCIPP list requires detailed information, such as latitude and longitude coordinates, that may not be available for assets with unique characteristics.

By contrast, most state officials we contacted reported that it is difficult to nominate assets to the NCIPP list using the consequence-based criteria, and two officials said that they are considering whether to continue to participate in the NCIPP process. Homeland security officials representing 13 of the 15 states told us that they believe that the nomination process is moderately difficult or very difficult, while officials representing 2 states told us that they believe the nomination process is neither easy nor difficult. For the 13 states where officials told us that they believe the nomination process is moderately difficult or very difficult, officials representing 5 states told us that not having the capability and resources to develop scenarios to support consequence-based criteria (such as conducting economic analysis) are the major factors contributing to the time-consuming and difficult process of submitting nominations when the criteria changed. Officials from 2 states told us that their states no longer plan to nominate infrastructure to the NCIPP list because of the time and effort required to make nominations.

[56] DHS accepts nominations made by two out of these five SSAs directly to the NCIPP list.

DHS Is Working to Address Challenges Facing States

DHS officials told us that they recognize that some states are facing challenges participating in the NCIPP program (as we previously identified in our discussions with state officials) and, according to officials, they are working to help them address some of these challenges. For example, DHS officials said that they recognized that the change to consequence-based criteria was difficult because it required states to invest considerable resources to make nominations. However, they also believe that other factors may influence states' willingness to participate, such as (1) some state officials may believe that all critical infrastructure has been captured for the state and sector, (2) some state officials may believe that the benefits of participating—such as access to grant funding—have diminished and there is no longer an incentive to participate, and (3) the NCIPP data call process is voluntary and state partners do not have to participate if they do not wish.

DHS has taken several steps to minimize the burden on state partners. First, DHS is conducting a more limited annual data call wherein all assets identified on the previous list are generally carried forward onto the subsequent list and states are asked to provide nominations of (1) critical infrastructure not accepted during the previous data call or (2) critical infrastructure not previously nominated but that partners believe merits consideration.[57] In fiscal year 2013, 13 state or territorial partners participated in the data call. DHS officials question whether, given current budget constraints facing state and federal partners, there is a need to conduct an annual data call. In our past work, we have reported that, with our nation facing serious, long-term fiscal challenges, a reevaluation of federal agencies' operations has never been more important than it is today.[58] Consistent with our past work, DHS officials told us that they considered whether the costs of conducting an annual data call outweigh the benefits, since only minor updates are being made to the NCIPP list. In addition, one state official observed that, in a resource-constrained environment, states can no longer afford to conduct the NCIPP data call because it diverts resources from critical infrastructure protection partnership and coordination activities that could increase state and regional resilience, such as states maintaining their own list of high-priority critical infrastructure. In response, according to DHS officials, DHS

[57] According to DHS officials, states and SSAs may request that DHS update or remove infrastructure on the previous year's NCIPP list during, or outside of, the annual data call.

[58] GAO-12-972.

is working to minimize major changes to the consequence-based NCIPP criteria, and thus, does not anticipate making any major changes to the NCIPP criteria that would cause a burden on state resources. Finally, DHS officials also told us that they have begun to take additional actions to enhance state participation, including developing and organizing a webinar with PSAs and state officials as they execute the data call. DHS is also working collaboratively with the State, Local, Tribal and Territorial Government Coordinating Council to develop a guide to assist states with their efforts to identify and prioritize their critical infrastructure.[59]

DHS Could Not Verify That It Met Requirements to Report to Congress on the NCIPP

DHS has prepared documents describing the national asset database and the prioritized critical infrastructure list; however, DHS could not verify that it has delivered these documents for purposes of meeting its statutory requirement to report this information to the congressional committees specified in the law. Pursuant to the 9/11 Commission Act, which amended title II of the Homeland Security Act, DHS is required 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 on, among other things, any significant challenges in compiling the database or list and, if appropriate, the extent to which the database or list has been used to allocate federal funds to prevent, reduce, mitigate, or respond to acts of terrorism.[60] Although DHS was able to compile documents on the database and list for fiscal years 2008 through 2011 that generally contain the information on which DHS is to report, officials from DHS and the Office of Infrastructure Protection told us they were uncertain whether the documents were delivered to the requisite congressional committees because they do not have records to indicate that the documents were delivered. According to a DHS official, the DHS document tracking system includes notes on the intended delivery of the fiscal year 2008 and 2010 documents and a note regarding delivery of the fiscal year 2009

[59] 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.

[60] See 6 U.S.C. § 124*l*(d).

document, but the system does not contain a record to verify that the documents were delivered, i.e., that the transactions actually occurred.[61] Staff from both committees could not find evidence of the documents. One staff member also conducted a search of congressional archives for the 109th, 110th, and 111th Congresses and found no records of receiving the statutorily required reports from DHS.

We reviewed the DHS documents intended to fulfill the statutory reporting requirements for fiscal years 2008 through 2011 and found that they generally contain information consistent with the statutory requirements. For example, the documents generally included an overview of the NCIPP list development process and changes, if any, from the previous year; challenges compiling the list; and how the list is used. Table 2 shows key elements of each document and how they match up with the statutory requirements.

Table 2: Comparison of Statutory Reporting Requirements and DHS Report Responses

	Document dates			
Statutory reporting requirements	**May 2008[a]**	**May 2009**	**June 2010**	**January 2011[a]**
Name, location, and sector of each system/asset on the list	✓	✓	✓	
Name, location, and sector of each system/asset on the list determined to be most at risk to terrorism	✓	✓	✓	
Any significant challenges in compiling the list of systems/assets included on the list or in the database	✓	✓	✓	✓
Any significant changes from the preceding report in the systems/assets included on the list or in the database	✓	✓	✓	
If appropriate, the extent to which the database or list has been used for allocating federal government funds to prevent, reduce, mitigate, or respond to acts of terrorism	✓	✓	✓	✓
Amount of coordination between DHS and the private sector for the purpose of ensuring the accuracy of the database and list	✓	✓	✓	✓

Source: GAO analysis of DHS documents.

[a]Draft documents have been provided for these years.

Nevertheless, absent an approach to verify the delivery of the statutorily required reports on the database and list to the requisite committees of Congress, DHS cannot ensure that it has provided the committees with

[61] The agency official told us that the fiscal year 2011 document is still in internal review and therefore has not been delivered to the requisite congressional committees.

necessary information in a timely manner. The *Standards for Internal Control in the Federal Government* calls for compliance with applicable laws and regulations and for the accurate, timely, and appropriate documentation of the transactions.[62] An approach to verify the timely delivery of required reports to the requisite committees of Congress, such as documenting or recording the transactions, would better position DHS to ensure that it is in compliance with its statutory reporting requirements, thereby providing the committees information needed to perform oversight.

Conclusions

DHS efforts to identify and prioritize infrastructure continue to evolve, and the department has taken important actions to focus its prioritization approach on consequences, consistent with statutory requirements and the NIPP risk management framework. However, in recent years, DHS introduced new criteria for select sectors and non-consequence-based criteria to account for some assets, which could hinder DHS's ability to compare assets across sectors in order to identify the nation's highest-priority critical infrastructure. Given the magnitude of the changes DHS has made to the criteria for including infrastructure on the list, validation of the NCIPP list development approach could provide DHS managers and infrastructure protection partners more reasonable assurance that the list captures the highest-priority infrastructure that, if destroyed or disrupted, could cause national or regional catastrophic effects. NCIPP program officials told us they would like to have the NCIPP reviewed to validate the criteria used to decide which assets and systems should be placed on the list, but they have not yet submitted a proposal for this review to the Assistant Secretary for Infrastructure Protection. An independent, external peer review would better position DHS to provide reasonable assurance that its approach is reproducible and defensible, and that infrastructure protection efforts are being prioritized on the nation's highest-priority critical infrastructure as intended by the NIPP risk management framework. Finally, it is unclear if DHS has met statutory annual reporting requirements regarding the NCIPP lists because DHS is unable to verify the delivery of these required reports. As a result, DHS cannot ensure that it is fulfilling its statutory reporting obligations and may not be providing the requisite congressional committees with the information

[62] See GAO/AIMD-00-21.3.1.

needed to effectively oversee the program, particularly with regard to the allocation of scarce federal resources.

Recommendations for Executive Action

To better ensure that DHS's approach to identify and prioritize critical infrastructure is consistent with the NIPP risk management framework and that DHS is positioned to provide reasonable assurance that protection and resiliency efforts and investments are focused on the nation's highest-priority critical infrastructure, we recommend that the Assistant Secretary for Infrastructure Protection, Department of Homeland Security, take the following action:

- commission an independent, external peer review of the program with clear project objectives for completing this effort.

To ensure that DHS is in compliance with its statutory reporting requirements and provides decision makers with the information necessary to perform program oversight, we recommend that the Secretary of Homeland Security, take the following action:

- develop an approach, such as documenting or recording the transaction, to verify the delivery of the statutorily required annual reports on the database and list to the requisite congressional committees.

Agency Comments and Our Evaluation

We provided a draft of this report to the Secretary of Homeland Security for review and comment. In its written comments reproduced in Appendix III, DHS agreed with both of our recommendations.

With regard to our first recommendation that DHS commission an independent, external peer review of the program with clear project objectives for completing this effort, DHS stated that a peer review would enable DHS to determine whether the NCIPP list is based on analytically sound methodology and whether appropriate procedures are in place to ensure that the list is defensible and reproducible. Specifically, DHS stated that it plans to commission and complete an independent peer review of the NCIPP process by the end of the fourth quarter of fiscal year 2014. If fully implemented, to include a review by independent experts to validate the criteria and process DHS uses to decide which assets and systems should be placed on the NCIPP list as we described in this report, DHS's planned efforts will address the intent of this recommendation.

With regard to our second recommendation that DHS develop an approach, such as documenting or recording the transaction, to verify the delivery of the statutorily required annual reports on the database and list to the requisite congressional committees, DHS stated that it has a system in place to track the development and approval of congressional reports, but DHS confirmed that it does not currently have a standard procedure for verifying that the congressional reports are delivered. DHS stated that its Office of Legislative Affairs will develop and implement a standard operating procedure for tracking the delivery of annual reports on the database and the list. DHS did not provide an estimated completion date for this effort. If fully implemented, DHS's planned efforts will address the intent of this recommendation.

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

We are sending copies of this report to the Secretary of Homeland Security, the Under Secretary of the National Programs Protection Directorate, selected congressional committees, and other interested parties. In addition, the report is available at no charge on GAO's website at http://www.gao.gov. If you or your staff have any questions about this report, please contact Stephen L. Caldwell at (202) 512-8777 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 are listed in appendix IV.

Steve Caldwell

Stephen L. Caldwell
Director, Homeland Security and Justice Issues

Appendix I: Critical Infrastructure Sectors

This appendix provides information on the 18 critical infrastructure 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 18 critical infrastructure sectors. Homeland Security Presidential Directive/HSPD-7 and the NIPP assign responsibility for critical infrastructure sectors to sector-specific agencies (SSA). On February 12, 2013, the President issued Presidential Policy Directive/PPD-21 that, among other things, reduced the number of critical infrastructure sectors from 18 to 16.[1] As an SSA, DHS has direct responsibility for leading, integrating, and coordinating efforts of sector partners to protect 11 of the 18 critical infrastructure sectors. The remaining sectors are coordinated by eight other federal agencies. Table 3 lists the SSAs and their sectors as they existed before any reorganization of the critical infrastructure sectors affected by the issuance of PPD-21.

[1] The directive also revoked HSPD-7 but provided that plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

Table 3: Sector-Specific Agencies (SSA) and Critical Infrastructure Sectors

SSA	Critical infrastructure sector
Department of Agriculture[a] and the Food and Drug Administration[b]	Agriculture and food
Department of Defense[c]	Defense industrial base
Department of Energy	Energy[d]
Department of Health and Human Services	Health care and public health
Department of the Interior	National monuments and icons
Department of the Treasury	Banking and finance
Environmental Protection Agency	Water[e]
Department of Homeland Security	
• Office of Infrastructure Protection	Commercial facilities Critical manufacturing Emergency services Nuclear reactors, materials, and waste Dams Chemical
• Office of Cyber Security and Communications	Information technology Communications
• Transportation Security Administration	Postal and shipping
• Transportation Security Administration and U. S. Coast Guard[f]	Transportation systems[g]
• Federal Protective Service[h]	Government facilities[i]

Source: GAO review of the 2009 *National Infrastructure Protection Plan* and other DHS documents.

Note: On February 12, 2013, the President issued Presidential Policy Directive/PPD-21 that, among other things, reduced the number of critical infrastructure sectors from 18 to 16. This table lists the SSAs and their sectors as they existed before any reorganization of the critical infrastructure sectors affected by the issuance of PPD-21.

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

[b] The Food and Drug Administration is part of the Department of Health and Human Services and is responsible for food other than meat, poultry, and egg products.

[c] 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.

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

[e] The water sector includes drinking water and wastewater systems.

[f] The U.S. Coast Guard is the SSA for the maritime transportation mode within the transportation systems sector.

[g] In accordance with HSPD-7, the Department of Transportation and the Department of Homeland Security are to collaborate on all matters relating to transportation security and transportation infrastructure protection.

[h] As of October 2009, the Federal Protective Service had transitioned out of U.S. Immigration and Customs Enforcement to the National Protection and Programs Directorate.

[i] The Department of Education is the SSA for the education facilities subsector of the government facilities sector.

Appendix II: Objectives, Scope, and Methodology

To address our first objective—determine the extent to which DHS changed its criteria for developing the National Critical Infrastructure Prioritization Program (NCIPP) list, identified the impact, if any, of these changes, and validated its approach—we reviewed the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), which, by amending title II of the Homeland Security Act of 2002, required the Secretary of DHS to establish and maintain a national database of systems and assets determined to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States, any state, or any local government, or as otherwise determined appropriate for inclusion by the Secretary.[1] In addition, the 9/11 Commission Act required the Secretary of DHS to establish and maintain a single prioritized list of systems and assets included in the national database that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects.[2]

We also reviewed DHS guidelines issued to states and SSAs from 2007 through 2012 that included details on the NCIPP list development process, to determine how DHS's criteria and process for developing the list changed year to year. We then obtained and analyzed the NCIPP lists finalized for fiscal years 2007 through 2012 to determine the total number of high-priority assets by state and the change in distribution of high-priority assets by sector year to year.[3] We used our analysis to select 8 of the 18 sectors—the banking and finance, defense industrial base, chemical, energy, transportation systems, agriculture and food, government facilities, and dams sectors. We chose these sectors to obtain a mix of sectors that (1) experienced the largest and smallest percentage change in the distribution of assets on the NCIPP list between fiscal years 2009 and 2011 because of program changes DHS made

[1] See 6 U.S.C. § 124*l*(a)(1).

[2] See 6 U.S.C. § 124*l*(a)(2).

[3] As described in our prior work (GAO-12-378), DHS was not previously recording NCIPP data—such as facility names—consistently. Thus, it was not possible to systematically analyze whether the same facilities are on the list from year to year. Because of this limitation, we rely on the distribution of assets by sector from year to year to demonstrate changes to the composition of the list.

during this period, and (2) have an SSA located within or outside DHS.[4] The information from our analysis of these sectors is not generalizable to the universe of all sectors. However, it provides valuable insights into yearly changes in the distribution of assets on the NCIPP list among a diverse group of sectors. On February 12, 2013, the President issued Presidential Policy Directive/PPD-21 that, among other things, reduced the number of critical infrastructure sectors from 18 to 16.[5] To assess the reliability of the data, we reviewed existing documentation about DHS's data system, which houses the data application used to create the NCIPP list, and spoke with knowledgeable agency officials responsible for maintaining the system and data application. While we determined that the data were sufficiently reliable to provide a general overview of the program, we included data limitations from our previous work in this report, where appropriate. We also interviewed officials in the Infrastructure Analysis and Strategy Division (IASD), which is part of the Office of Infrastructure Protection in DHS's National Protection and Program Directorate, who are responsible for managing the NCIPP to identify DHS's rationale for changing the criteria.[6]

In addition, to address the first objective, we reviewed our prior reports as well as DHS Inspector General reports on protection and resiliency prioritization efforts and spoke with program officials who use the list from DHS's Protective Security Coordination Division (PSCD), the Federal Emergency Management Agency (FEMA), and the Federal Bureau of Investigation to determine how they use the NCIPP list and the impact changes to the NCIPP list have had, if any, on their ability to use the list

[4] Because of the challenges encountered with changes DHS made to the NCIPP criteria in 2009, the fiscal year 2010 NCIPP list was not approved by the Assistant Secretary for Infrastructure Protection and therefore not finalized or used. Additionally, the precise number of assets on the NCIPP list is information that DHS designated "for official use only." We have not included this information in this report so that we could publicly present the results of our work.

[5] The directive also revoked HSPD-7 but provided that plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded. This does not affect our review because we began and conducted the bulk of our work prior to the release of this directive.

[6] In May 2012, we reported that the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) coordinated the NCIPP. HITRAC is an office within IASD. See GAO, *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments*, GAO-12-378 (Washington, D.C.: May 31, 2012).

during fiscal years 2007 through 2012.[7] In addition to interviewing program officials from PSCD headquarters, we also conducted interviews with nine of DHS's protective security advisors (PSA)—one from each of the nine PSA regions—to discuss their contributions to the NCIPP list, how they use the list to prioritize their activities, and actions NCIPP management has taken to solicit their feedback regarding the program.[8] The results from our interviews are not generalizable to the universe of PSAs but provide specific examples of how PSAs use the list and insights on the effect changes have had on their activities.

We also conducted a sensitivity analysis using the FEMA Urban Area Security Initiative (UASI) grant risk formula to determine the smallest possible change needed in the NCIPP infrastructure count inputs that would result in a change to the relative risk score rankings of the top 31 cities that received UASI grant funds in fiscal year 2012.[9] Specifically, we applied a random number generator bounded by -2 and +2 to the NCIPP level 2 infrastructure counts that were used as an input to the risk formula

[7] For example, see GAO-12-378; GAO, *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operation*s, GAO-12-14 (Washington, D.C: Nov. 17, 2011); DHS OIG-09-86 *Efforts to Identify Critical Infrastructure Assets and Systems*, (Washington, D.C.: June 2009); and DHS OIG-06-40 *Progress in Developing the National Asset Database*, (Washington, D.C.: June 2006).

[8] PSAs are DHS field representatives responsible for, among other things, conducting voluntary security surveys and vulnerability assessments on NCIPP-listed assets and other critical infrastructure. During the course of our review, DHS realigned the PSA regions to match the standard federal regions (i.e., the 10 FEMA regions). However, for the purpose of our review, which began prior to the realignment, the PSA regions were the National Capital Region, Great Lakes Area, Gulf Coast Area, Mid-Atlantic Area, Midwest Area, Northeast Area, Northwest Area, Southeast Area, and Southwest Area.

[9] Although the FEMA UASI grant formula is the same as the FEMA State Homeland Security Program (SHSP), we focused our sensitivity analysis on the UASI grant because this grant is allocated to only a subset of the nation's 100 most populous urban areas—referred to as metropolitan statistical areas (MSA)—each year, whereas by law, each state and territory are required to receive a minimum allocation of the SHSP funds each year. For ease of reporting, we will refer to UASI grant recipients as cities rather than MSAs.

for these 31 cities.[10] We then re-ran the risk formula using these revised NCIPP level 2 infrastructure counts, while holding all other data inputs constant, which resulted in a change to the relative risk score rankings for 5 of the top 31 cities. We also performed additional statistical analysis of the FEMA risk formula and data that showed UASI grant allocations are strongly associated with a city's current risk score, even when accounting for the influence of the previous year's grant allocations. Based on our prior work with the FEMA UASI grant risk formula and interviews with FEMA officials about its data sources and quality assurance procedures, we determined that the data were sufficiently reliable for the purposes of this report.[11] Last, we met with IASD officials to discuss actions they have taken to identify the impact of changes, if any, on users of the list, and compared these actions with applicable criteria in the NIPP and *Standards for Internal Control in the Federal Government* to determine if they were consistent.[12]

Regarding our second objective—to determine the extent to which DHS worked with states and SSAs to develop the NCIPP list—we reviewed relevant provisions of the 9/11 Commission Act and the guidelines DHS issued to state homeland security advisers and SSAs to solicit nominations of high-priority infrastructure for inclusion on the NCIPP list.

[10] We focused our experiment on NCIPP level 2 infrastructure counts because (1) level 2 counts are much higher since only a small portion of the NCIPP list is composed of level 1 assets and (2) the FEMA grant model values level 1 assets more than it does level 2 assets, so a change to level 2 counts represents a smaller change to the model consistent with the purpose of our experiment. Additionally, the same experiment using a random number generator bounded by -1 and +1 resulted in no change in the relative risk score rankings of the top 31 cities.

[11] See GAO-12-303 and GAO, *Homeland Security: DHS Risk-Based Grant Methodology Is Reasonable, but Current Version's Measure of Vulnerability Is Limited*, GAO-08-852 (Washington D.C.: June 27, 2008).

[12] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD 00-21.3.1 (Washington, D.C.: November 1999). Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982 (FMFIA), provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to FMFIA, the Office of Management and Budget issued Circular A-123, revised December 21, 2004, to provide the specific requirements for assessing the reporting on internal controls. Internal control standards and the definition of internal control in Circular A-123 are based on GAO's *Standards for Internal Control in the Federal Government*.

We also conducted interviews with officials from 10 SSAs and 15 state homeland security offices to obtain federal and state perspectives on DHS's change to consequence-based criteria and coordination of the NCIPP program, as well as their views on nominating to and using the list. The SSA officials we interviewed represented the 8 sectors selected during our analysis for the first objective. Specifically, DHS was the SSA for 4 of the sectors—the chemical, dams, government facilities, and transportation systems sectors.[13] The Departments of Energy, Defense, and the Treasury were the SSAs for 3 sectors—the energy, defense industrial base, and banking and finance sectors, respectively. Two SSAs, the Department of Agriculture and the Food and Drug Administration, share responsibility for the agriculture and food sector. The state homeland security officials we interviewed represented 15 states—California, Georgia, Illinois, Hawaii, Oklahoma, Maine, Mississippi, Nevada, New Jersey, New York, Texas, Virginia, Washington, West Virginia, and Wisconsin. We selected these states because they contained a range in the number of assets on the NCIPP list and represented at least 1 state from each of 9 PSA regions.[14] The sector and state interviews are not generalizable to the universe of infrastructure sectors and states contributing to the NCIPP list. However, our selection combined with DHS policy guidance, further informed us about DHS efforts to manage the NCIPP program across a spectrum of states and partners nationwide. Finally, we interviewed IASD officials to discuss actions DHS had taken to consult with state and federal partners (as identified in program guidelines and based on our interviews with states and SSAs), and compared their responses with applicable criteria in the NIPP, *Standards for Internal Control in the Federal Government*, and relevant statutory provisions.

With regard to our third objective—determine the extent to which DHS reported to the requisite committees of Congress on the NCIPP—we reviewed the statutory requirement that DHS report annually to the Senate Committee on Homeland Security and Governmental Affairs and

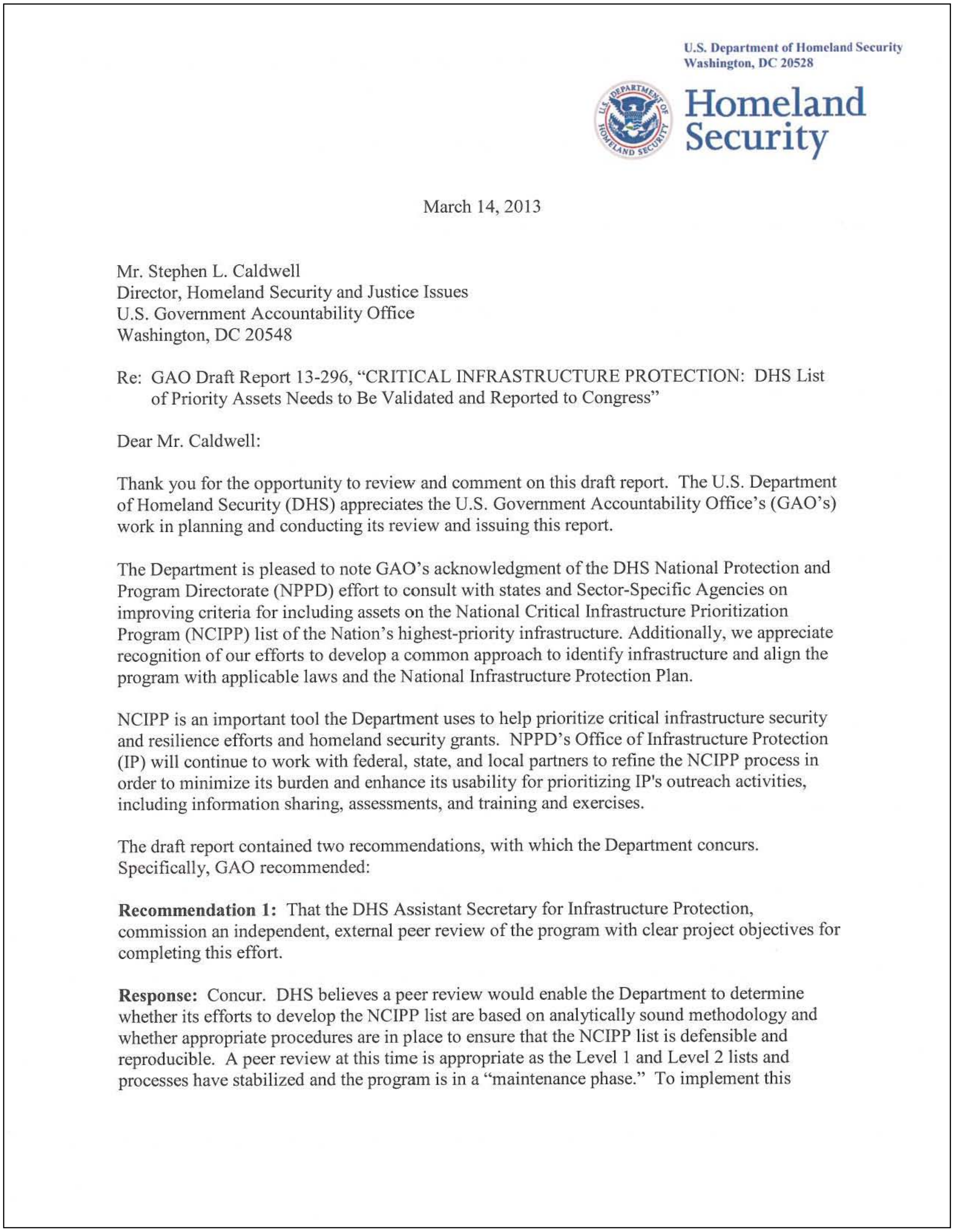
[13] Two DHS components are the SSAs for the transportation systems sector: the Transportation Security Administration and the U.S. Coast Guard.

[14] For the purposes or our review, we selected states that contained a mix of smaller, medium-sized, and larger numbers of assets on the list. The precise number of assets on the NCIPP list is information that DHS designated "for official use only." We have not included this information in this report so that we could publicly present the results of our work.

the House Committee on Homeland Security on the national asset database and prioritized critical infrastructure list. We also spoke to staff members representing both committees to determine if the committees received the statutorily required reports. Last, we interviewed DHS officials to discuss efforts to provide these reports to the committees and obtained and reviewed documents on the national asset database and prioritized critical infrastructure list that were intended to meet statutory reporting requirements to determine if these efforts were consistent with relevant statutory provisions and *Standards for Internal Control in the Federal Government*.

We conducted this performance audit from May 2012 to March 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.

Appendix III: Comments from the Department of Homeland Security



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

Homeland Security

March 14, 2013

Mr. Stephen L. Caldwell
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
Washington, DC 20548

Re: GAO Draft Report 13-296, "CRITICAL INFRASTRUCTURE PROTECTION: DHS List of Priority Assets Needs to Be Validated and Reported to Congress"

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.

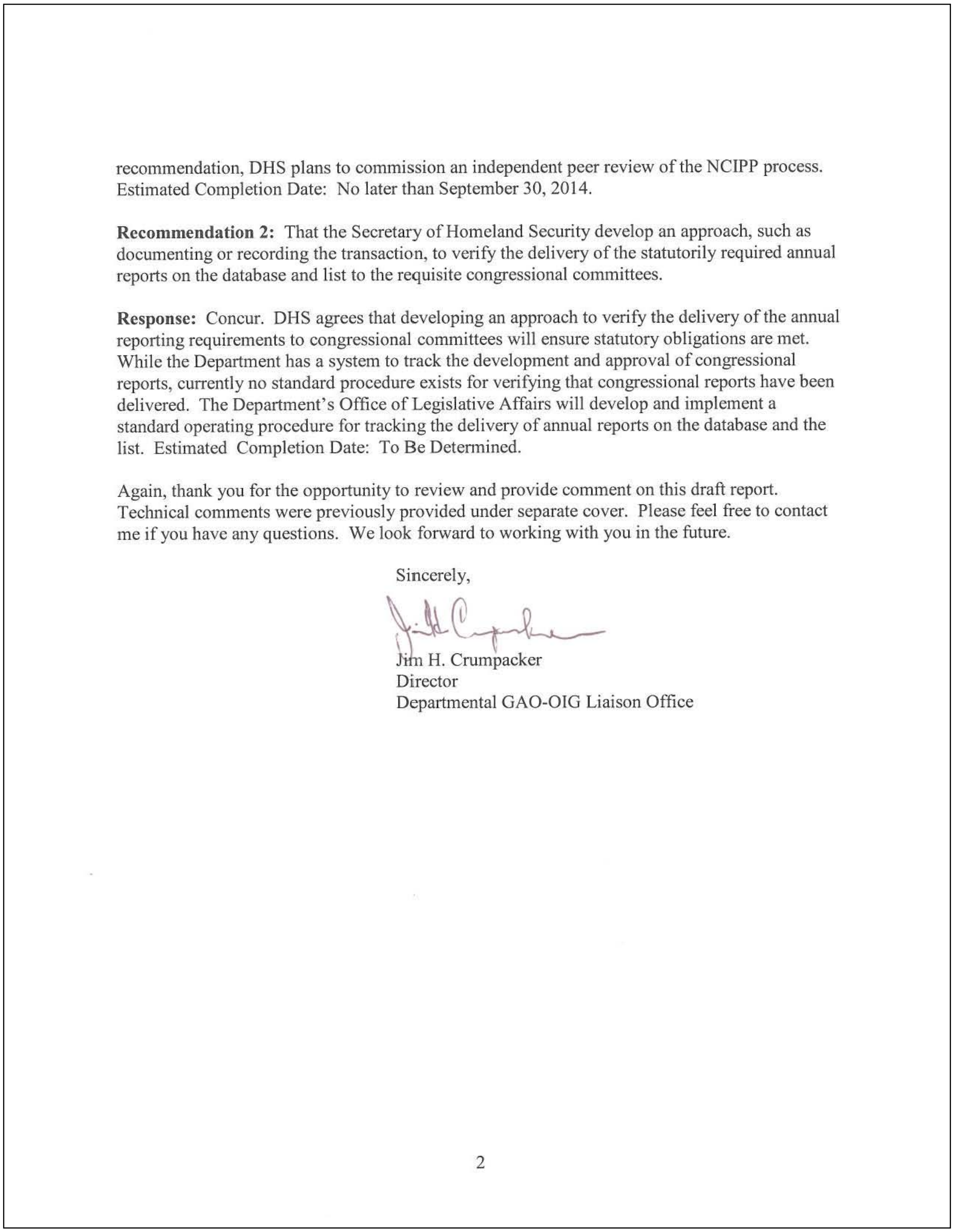
The Department is pleased to note GAO's acknowledgment of the DHS National Protection and Program Directorate (NPPD) effort to consult with states and Sector-Specific Agencies on improving criteria for including assets on the National Critical Infrastructure Prioritization Program (NCIPP) list of the Nation's highest-priority infrastructure. Additionally, we appreciate recognition of our efforts to develop a common approach to identify infrastructure and align the program with applicable laws and the National Infrastructure Protection Plan.

NCIPP is an important tool the Department uses to help prioritize critical infrastructure security and resilience efforts and homeland security grants. NPPD's Office of Infrastructure Protection (IP) will continue to work with federal, state, and local partners to refine the NCIPP process in order to minimize its burden and enhance its usability for prioritizing IP's outreach activities, including information sharing, assessments, and training and exercises.

The draft report contained two recommendations, with which the Department concurs. Specifically, GAO recommended:

Recommendation 1: That the DHS Assistant Secretary for Infrastructure Protection, commission an independent, external peer review of the program with clear project objectives for completing this effort.

Response: Concur. DHS believes a peer review would enable the Department to determine whether its efforts to develop the NCIPP list are based on analytically sound methodology and whether appropriate procedures are in place to ensure that the NCIPP list is defensible and reproducible. A peer review at this time is appropriate as the Level 1 and Level 2 lists and processes have stabilized and the program is in a "maintenance phase." To implement this



recommendation, DHS plans to commission an independent peer review of the NCIPP process. Estimated Completion Date: No later than September 30, 2014.

Recommendation 2: That the Secretary of Homeland Security develop an approach, such as documenting or recording the transaction, to verify the delivery of the statutorily required annual reports on the database and list to the requisite congressional committees.

Response: Concur. DHS agrees that developing an approach to verify the delivery of the annual reporting requirements to congressional committees will ensure statutory obligations are met. While the Department has a system to track the development and approval of congressional reports, currently no standard procedure exists for verifying that congressional reports have been delivered. The Department's Office of Legislative Affairs will develop and implement a standard operating procedure for tracking the delivery of annual reports on the database and the list. Estimated Completion Date: To Be Determined.

Again, thank you for the opportunity to review and provide comment 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

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen L. Caldwell, (202) 512-8777 or caldwells@gao.gov

Staff Acknowledgments

In addition to the contact named above, John F. Mortin, Assistant Director, and Andrew M. Curry, Analyst-in-Charge, managed this assignment. Chuck Bausell, Mona Nichols-Blake, Aryn Ehlow, Katherine M. Davis, Michele C. Fejfar, Eric D. Hauswirth, Mitchell B. Karpman, Thomas F. Lombardi, and Janay Sam made significant contributions to the work.

Related GAO Products

Critical Infrastructure Protection: Preliminary Observations on DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach. GAO-13-421T. Washington, D.C.: March 14, 2013.

Critical Infrastructure Protection: An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure. GAO-13-11. Washington, D.C.: October 25, 2012.

Critical Infrastructure Protection: Summary of DHS Actions to Better Manage Its Chemical Security Program. GAO-12-1044T. Washington, D.C.: September 20, 2012.

Critical Infrastructure Protection: DHS Is Taking Action to Better Manage Its Chemical Security Program, but It Is Too Early to Assess Results. GAO-12-567T. Washington, D.C.: September 11, 2012.

Critical Infrastructure: DHS Needs to Refocus Its Efforts to Lead the Government Facilities Sector. GAO-12-852. Washington, D.C.: August 13, 2012.

Critical Infrastructure Protection: DHS Is Taking Action to Better Manage Its Chemical Security Program, but It Is Too Early to Assess Results. GAO-12-515T. Washington, D.C.: July 26, 2012.

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

Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities. GAO-11-537R. Washington, D.C.: May 19, 2011.

Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened. GAO-10-772. Washington, D.C.: September 23, 2010.

Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience. GAO-10-296. Washington, D.C.: March 5, 2010.

The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report. GAO-09-654R. Washington, D.C.: June 26, 2009.

Information Technology: Federal Laws, Regulations, and Mandatory Standards to Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors. GAO-08-1075R. Washington, D.C.: September 16, 2008.

Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security. GAO-08-904T. Washington, D.C.: June 25, 2008.

Critical Infrastructure: Sector Plans Complete and Sector Councils Evolving. GAO-07-1075T. Washington, D.C.: July 12, 2007.

Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve. GAO-07-706R. Washington, D.C.: July 10, 2007.

Critical Infrastructure: Challenges Remain in Protecting Key Sectors. GAO-07-626T. Washington, D.C.: March 20, 2007.

Homeland Security: Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks. GAO-07-375. Washington, D.C.: January 24, 2007.

Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics. GAO-07-39. Washington, D.C.: October 16, 2006.

Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information. GAO-06-383. Washington, D.C.: April 17, 2006.

Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. GAO-06-91. Washington, D.C.: December 15, 2005.

(441076)