Department of Homeland Security
Office of Inspector General

Efforts to Identify Critical Infrastructure Assets and Systems

OIG-09-86

June 2009

Office of Inspector General

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

June 30, 2009

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses Department of Homeland Security identification and use of critical infrastructure asset and systems data. We based our report on interviews with relevant agencies, direct observations, and a review of applicable documents and data.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all who contributed to the preparation of this report.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Table of Contents/Abbreviations

Abbreviations

ACAMS	Automated Critical Asset Management System
CIKR	Critical Infrastructure/Key Resources
CIO	Chief Information Officer
DHS	Department of Homeland Security
DIB	Defense Industrial Base
EAB	Enterprise Architecture Board
FASCAT	Food and Agriculture Sector Criticality Assessment Tool
FEMA	Federal Emergency Management Agency
GAO	Government Accountability Office
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
ICE	Immigration and Customs Enforcement
IDW	Infrastructure Data Warehouse
IICS	Infrastructure Information Collection System
IP	Office of Infrastructure Protection
IRB	Investment Review Board
NADB	National Asset Database
NIAC	National Infrastructure Advisory Council
NII	National Infrastructure Index
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NPPD	National Protection and Programs Directorate
NSI	National Security Index
OIG	Office of Inspector General
PSA	Protective Security Advisor
SHSP	State Homeland Security Program
SSA	Sector Specific Agency
TSA	Transportation Security Administration
UASI	Urban Area Security Initiative

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

This report fulfills a statutory requirement from Section 1001 of the *Implementing Recommendations of the 9/11 Commission Act* that requires the Office of Inspector General to review the Department of Homeland Security's (DHS) efforts to identify critical infrastructure. Efforts to catalog the nation's critical assets and systems are important steps to satisfying the departmental mission of securing the homeland. Our June 2006 report, *Progress in Developing the National Asset Database* (OIG-06-40), examined early DHS work in this area.

The National Protection and Programs Directorate is in the process of acquiring the Infrastructure Information Collection System, a replacement for the National Asset Database. Staff in the directorate expressed several concerns about the acquisition process. Additional interaction between these staff experts and the Directorate of Management offers the possibility of greater cooperation in acquiring the new system and hiring employees.

The primary means used to identify the nation's most critical assets and systems is the annual Prioritized Critical Infrastructure List process. The department works with public and private sector experts to create the two lists, which are designed to identify the nation's most critical assets and systems. The lists provide a reasonable means to fulfill statutory mandates, DHS critical infrastructure goals, and overall risk management activities. Public and private sector experts expressed appreciation for DHS efforts to work with partners throughout critical infrastructure identification efforts. We determined that some changes in this DHS effort would enhance efficiency, expand partnerships, and gain more resources to improve the process on an ongoing basis.

We are making 10 recommendations to improve DHS efforts to identify and catalog critical infrastructure assets and systems.

Background

DHS must work with an array of public and private sector stakeholders to identify the nation's critical infrastructure. This section describes DHS asset identification efforts and the partnership model established in the National Infrastructure Protection Plan (NIPP), which was revised in 2009. The NIPP lists DHS infrastructure protection goals.

Overview of Asset Identification Efforts

DHS is responsible for leading the national effort to identify and protect critical infrastructure. The *National Strategy for Homeland Security* specifies critical infrastructure and key resources (CIKR) protection as one of four DHS significant mission goals.[1] Since 1998, several policies and strategies have established the protection of the nation's CIKR as vital to securing the homeland. According to the NIPP, one of the initial steps to protect the nation's infrastructure is to "identify assets, systems, networks, and functions."[2] Asset identification is an essential preliminary step to knowing the extent of the nation's CIKR for purposes of targeting grant funding and other efforts.

Section 1001 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (hereinafter "The Act") mandates that DHS maintain and use a database to catalog the nation's critical infrastructure. We are required to review the department's implementation of Section 1001.[3]

DHS is required to develop a comprehensive system that catalogs critical infrastructure and enhances CIKR protection.[4] Previously, DHS inventoried assets, systems, networks, and functions through the National Asset Database (NADB). In June 2006, we reported that the NADB did not distinguish assets by criticality. The department countered with the assertion that the database was not intended to be a list of critical assets. The divergence of opinion

[1] Homeland Security Council, *National Strategy for Homeland Security*, October 2007, p. 1.
[2] Department of Homeland Security, *National Infrastructure Protection Plan*, 2006, p. 4.
[3] *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53), § 1001.
[4] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003, p. 23.

on the purpose of the NADB created confusion in Congress and the media.[5]

DHS asset identification efforts must catalog systems or assets that would have “a negative or debilitating effect” on the United States if disrupted or attacked. The Prioritized Critical Infrastructure List, another asset cataloging instrument to identify the nation’s most critical assets and systems, is also required.[6] DHS is therefore charged to create both a general database of critical infrastructure and a list of the nation’s most important assets and systems. DHS must report annually to Congress regarding progress and difficulties encountered in identifying and collecting CIKR information.

DHS policy maintains that CIKR information repositories will inform decision making and specific response and recovery activities.[7] Thus, any system to catalog national assets must provide a comprehensive overview of critical infrastructure. At the end of 2006, DHS discontinued operational use of the NADB. The DHS Office of Infrastructure Protection (IP) is now acquiring the Infrastructure Information Collection System (IICS). One component of the IICS is the Infrastructure Data Warehouse (IDW), which will replace the NADB. This new data system will allow relevant critical infrastructure partners from federal, state, local, and private entities to access various tools that house infrastructure data. The information in the IDW will help DHS conduct further risk analysis and meet the national data management requirements in Section 1001 of the Act. Our review focused on plans for the IDW and issues related to the procurement of the IICS. We did not conduct a detailed review of all planned components of the IICS.

Because the IICS is still in development, the primary DHS effort to identify critical infrastructure is the annual National Critical Infrastructure Prioritization Program. Delays in acquiring the IDW have meant that the lists created under the Program are not yet part of a national database, as the Act requires. Through the use of established criteria, states and sector experts provide DHS with lists of the nation’s most critical assets and systems.

[5] Congressional Research Service, *Critical Infrastructures: Background, Policy, and Implementation*, updated October 10, 2008, p. 28–29.
[6] P.L. 110-53, § 1001(a)(1)(A).
[7] DHS, *National Infrastructure Protection Plan*, p. 155.

The Sector Partnership Model

The elements of the nation's CIKR are divided into 18 sectors. Each sector has a federal agency, known as a Sector Specific Agency (SSA), designated to coordinate work across the private sector and all levels of government. The sectors and corresponding SSAs are listed in Table 1.

Table 1. Sectors and the Sector Specific Agencies

Sector	Sector Specific Agency
Agriculture and Food	Department of Agriculture and Department of Health and Human Services
Banking and Finance	Department of the Treasury
Chemical	DHS, Office of Infrastructure Protection
Commercial Facilities	DHS, Office of Infrastructure Protection
Communications	DHS, Office of Cyber Security and Communications
Critical Manufacturing	DHS, Office of Infrastructure Protection
Dams	DHS, Office of Infrastructure Protection
Defense Industrial Base	Department of Defense
Emergency Services	DHS, Office of Infrastructure Protection
Energy	Department of Energy
Government Facilities	DHS, Federal Protective Service
Information Technology	DHS, Office of Cyber Security and Communications
National Monuments and Icons	Department of Interior
Nuclear	DHS, Office of Infrastructure Protection
Postal and Shipping	DHS, Transportation Security Administration
Public Health and Healthcare	Department of Health and Human Services
Transportation	DHS, Transportation Security Administration and Coast Guard
Water	Environmental Protection Agency

DHS has created a sector partnership model designed to ensure communication between DHS, the SSAs, other federal agencies, state and local officials, and the private sector. The partners are as follows:

- Five DHS agencies that serve as SSAs;
- Seven non-DHS SSAs;
- State, local, and tribal governments; and
- The private sector.

Each sector operates a Government Coordinating Council, which includes public sector representatives who work with DHS. Sector Coordinating Councils ensure that DHS receives input from asset owners and trade associations. The Councils assess actions taken to identify CIKR and improve the protected status of assets and systems.[8] Protective Security Advisors (PSAs) are DHS's field-deployed infrastructure protection experts who interact and coordinate with Federal, State, local, territorial and tribal organizations and the private sector to assess and enhance the security of CIKR. There are currently 92 PSAs in all 50 States and Puerto Rico.

DHS has the overall responsibility to "lead, integrate, and coordinate" national critical infrastructure protection efforts.[9] Within DHS, IP is charged to carry out this mission. To accomplish this, IP must work with its CIKR partners, as described in the *National Strategy for Homeland Security*:

> "*While the Federal Government provides overarching leadership and coordination for protecting and mitigating vulnerabilities of our Nation's CIKR, all partners have important roles to play.*" [10]

IP recognizes that identification and prioritization of the nation's CIKR depends on the contributions and cooperation of its public and private sector stakeholders. The private sector, which owns most key assets and systems, has a vital role. Each SSA has unique knowledge and expertise. State, local, and tribal governments are also important partners.[11]

Results of Review

The plans for the IDW and the existing National Critical Infrastructure Prioritization Program are reasonable efforts to meet statutory requirements for identification of the nation's most critical infrastructure. DHS, however, is in the early stages of acquiring the IDW. As a result, the primary DHS effort to identify assets and systems is the annual lists of the nation's most critical infrastructure. The lists guide DHS grant allocation decisions and other risk management activities. IP has shown commendable interest in ongoing improvement to the list process. Our recommendations focus on ways IP could improve the identification of CIKR, increase partner participation, and obtain additional resources to enhance asset and system identification efforts.

[8] DHS, *National Infrastructure Protection Plan*, chapter 4.
[9] Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization and Protection," June 17, 2004.
[10] The Homeland Security Council, *National Strategy for Homeland Security*, October 2007, p. 28.
[11] DHS, *National Infrastructure Protection Plan*, chapter 2.

The Infrastructure Information Collection System Is in the Early Stages of Development

In September 2006, DHS leadership decided to suspend use of the NADB. IP staff stated that the database needed a variety of dynamic functions. The NADB was a static list of assets that did not link to mapping or analytical tools, which enhance a user's understanding of an asset and the effects of attacks or disruptions. As a replacement, DHS is acquiring the IDW, part of the IICS. The IDW will allow DHS and its CIKR partners to access a range of existing critical infrastructure information data sources more easily. DHS believes that the IDW will allow more rapid risk management across the infrastructure sectors, with the added advantage of decreased data maintenance costs and inefficiencies.

IP staff said that IICS will provide needed enhancements. As part of the IICS, the IDW would provide a single virtual view of one or more infrastructure data sources. The static nature of the NADB platform did not allow for such functionality. Experts in IP said that the integration of various data sources will be the prominent benefit of the IDW compared to the NADB. The IDW will offer users more information and provide benefits that will include a prompt means to assess natural or intentional disasters. DHS staff views the IDW as a significant restructuring of DHS CIKR identification activities.

DHS has identified four capability gaps in current critical infrastructure risk management. These gaps are the need for

1. Accessible and quantifiable risk-related information;
2. Data standards to ensure consistent data;
3. Common information collection and maintenance processes; and
4. Information fusion to enable current and complete analysis.

The department's May 2008 Report to Congress stated that these gaps restrict cross-sector and national risk analysis that use geographic data and other sources. The IDW is expected to diminish or eliminate these gaps.

Because the IDW is not fully developed, the Automated Critical Asset Management System (ACAMS) currently contributes to critical infrastructure asset identification. IP staff describes ACAMS as "the most mature operational information collection tool" in use. ACAMS will be the "cornerstone" of the IICS. A growing number of states and territories use ACAMS to collect infrastructure information and catalog assets. Although we noted difference of opinion among state officials, ACAMS is generally seen as a helpful tool to identify assets, gain further information about important sites, and target protective measures. We were informed of problems with inconsistent ACAMS data submission across states. We view these inconsistencies as inherent to a national process that focuses on submissions from 56 state and territorial governments.

Although ACAMS currently collects infrastructure information, IP officials have been frustrated with difficulties in hiring new employees and acquiring the IDW as part of the IICS. IP officials argue that the Directorate of Management's oversight requirements and evolving guidance contributed to problems with the IICS effort. IP staff said that these issues impede project management and prevent mission accomplishment. An IP manager lamented that the "centralized planning, centralized execution" paradigm hinders IP's ability to attract employees and efficiently procure technology.

IP management provided timelines and other information to illustrate concerns related to personnel security processing and the hiring process. IP staff noted that hiring delays have hindered development of the IDW. National Protection and Programs Directorate (NPPD) components such as IP rely on the department's Personnel Security Division for these functions. IP managers found the process frustrating and burdensome, from the time required to bring new staff on board to the transfer of security information for employees who already hold clearances. We did not analyze the directorate's personnel security issues for this report. However, our office recently reviewed the department's overall personnel security practices.[12] That report included various recommendations designed to improve overall efficiency and help DHS components add staff more expeditiously.

We received data from NPPD regarding the information technology acquisition process. Along with the Government Accountability Office (GAO), we have identified problems with the DHS acquisition function.[13] With extremely challenging and critical missions, DHS faces inherent procurement difficulties across varied components. The Office of Procurement Oversight division that covers NPPD had only 11 staff, yet was involved in more than 500 procurement requests in FY 2008.

IP staff had concerns with the department's Enterprise Architecture Board (EAB) and Investment Review Board (IRB). The EAB and IRB acquire key portions of DHS information technology. The primary purpose of the

[12] DHS OIG, *The DHS Personnel Security Process*, OIG-09-65, May 2009.
[13] GAO, *Department of Homeland Security: A Strategic Approach Is Needed to Better Ensure the Acquisition Workforce Can Meet Mission Needs*, GAO-09-30, November 2008; GAO, *Progress and Challenges in Implementing the Department's Acquisition Oversight Plan*, GAO-07-900, June 2007.

EAB is to ensure that component IT projects align with DHS missions and do not duplicate existing functions. The EAB also works to eliminate duplicative purchases. The IRB is composed of senior officials from DHS components who review major department investments.

In a July 2004 report, we highlighted concerns with these DHS boards.[14] We determined that the EAB does not provide a venue for including business perspectives on IT decisions, while the IRB postponed or cancelled 12 of 21 meetings. The IRB included high-level membership with competing priorities that had no sense of urgency. GAO also has reported problems that continue to diminish the effectiveness of the IRB.[15]

We concluded that the DHS Chief Information Officer (CIO) has been unable to "ensure that major IT investment reviews are conducted in a timely manner."[16] In September 2008, we reported that the DHS CIO is now "better positioned to meet the department's IT challenges." The report noted that the DHS CIO had an enhanced ability to oversee the investment review process. Refinements to the IRB and the applicable DHS Management Directive were also ongoing. Challenges remain, including CIO staffing shortages, limited CIO authority, and general acquisition review weaknesses.[17]

IP managers believe that problems with DHS oversight boards have affected the development of the IICS. Officials in the Directorate of Management have recognized problems with DHS IT acquisition oversight and procurement limitations. However, Directorate of Management officials said that oversight is needed to ensure that components' decisions do not adversely impact DHS missions. A recent GAO report on investment management recommended that DHS ensure that "components have established processes to manage major investments consistent with departmental policies."[18]

Directorate of Management staff noted that NPPD has experienced difficulties in its IT management, including a year-long vacancy in the NPPD CIO position, which was filled in October 2008. Moreover, NPPD

[14] DHS OIG, *Improvements Needed to DHS' Information Technology Management Structure*, OIG-04-30, July 2004.

[15] GAO, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversigh*t, GAO-09-29, November 2008.

[16] DHS OIG, *Improvements Needed to DHS' Information Technology Management Structure*, OIG-04-30, July 2004.

[17] DHS OIG*, Progress Made In Strengthening DHS Information Technology Management, But Challenges Remain*, OIG-08-91, September 2008.

[18] GAO-09-29, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversigh*t November 2008, p. 32.

has faced reorganizations and staffing problems. A Directorate of Management review of the IICS was completed in November 2007. This review cited significant planning, staffing, and program execution issues. IP officials responded that many of the deficiencies were outside the office's control, but corrective actions were continuing. Based on information obtained from DHS enterprise architecture and procurement managers, we concluded that NPPD has made a good faith effort to fulfill acquisition process mandates.

During fieldwork, we learned that the IP plans for the IDW are not well understood. The Director of Management's procurement chief in charge of NPPD acquisitions had not seen the IDW referenced before we contacted the office. Also, the department's security partners in the sectors and states have limited understanding of DHS goals for the IDW or how the new system will improve infrastructure risk management. Several sector experts were unfamiliar with the IDW concept, or first heard about plans for the IDW when IP managers asked SSAs to comment on IP's May 2008 Report to Congress.

The NADB has not been used as an operational system for more than 2 years; minimal progress has been made to finalize a more dynamic replacement. The new NPPD CIO should make the IICS acquisition process a priority. Assistance from the Directorate of Management would facilitate the NPPD CIO's efforts. Expanded leadership involvement could also explore solutions to IP's hiring problems. The IDW has the potential to enhance critical infrastructure protection, one of the department's strategic goals. Improved interaction between NPPD and the Directorate of Management is necessary to ensure that the IDW is procured in a way that meets departmental goals and satisfies the statutory requirement to catalog critical infrastructure.

We recommend that the Under Secretary for National Protection and Programs and the Under Secretary for Management:

> **Recommendation #1:** Complete the acquisition process for the Infrastructure Information Collection System.

The Prioritized Critical Infrastructure Lists Are the Primary Means Used to Identify Critical Infrastructure

Purpose of the List Process

The IDW is envisioned as the primary forum for information about infrastructure assets and systems. DHS also works to identify assets and systems that are deemed nationally critical through the National Critical Infrastructure Prioritization Program. Through work with states and the sectors, DHS creates the two lists of the most nationally significant infrastructure. These two lists are used for State Homeland Security Program and the Urban Area Security Initiative grant allocations. Additionally, the process is used to identify assets eligible for the Buffer Zone Protection Program (BZPP). This program is designed to increase security in the area outside a facility that can be used to conduct surveillance or launch an attack. Public and private sector security partners can also use the lists to prioritize infrastructure protection resources and conduct planning and coordination efforts.

The process, which is managed by the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), began in 2006. Successful interaction with states and the infrastructure sectors is a vital component of the process. Criticality criteria generated by the sectors and states, along with IP-produced consequence-based criticality thresholds, identifies the nation's most critical infrastructure. Because the criteria guide sector and state submissions of assets and systems, noncritical assets are less likely to be submitted. Critical infrastructure partners use the criteria to compile asset and systems information for each sector. Each year, the IP Assistant Secretary gives final approval of the lists.

Because the Act requires that the lists be part of the larger asset database, IP officials said that the lists will become part of the IDW. The process to create the lists is logically organized, with DHS partners seeing ongoing improvements in DHS' management of the lists. With some recommended improvements, the lists can provide additional support for CIKR identification, protection, and incident management efforts.

List Development

We reviewed information related to the lists for fiscal years 2006 to 2009. Significant changes were made for the 2009 process. One constant is that only two lists identify the nation's most critical assets and systems. These lists address the statutory requirement of a focus on prioritized critical infrastructure. The "Type 1" list includes infrastructure that if disrupted would have the highest consequence to the nation. A larger "Type 2" list includes all CIKR on the "Type 1" list and additional CIKR that if disrupted would have nationally significant consequences. According to IP officials, attacks against assets and systems on the

Type 1 list could have catastrophic national consequences. Attacks on assets on the Type 2 list would have nationally significant consequences. Our field work was based partners' impressions of the process prior to 2009, but we have included a description of the new process.

The 2009 process includes several enhancements. First, the two lists of nationally critical infrastructure are now completely based on consequence, rather than data such as asset size or seating capacity. Second, the concept of "critical clusters" has been introduced. This change identifies groups of related infrastructure that could be impacted by a single hazard. A cluster could rise to the level of national criticality, which would lead to inclusion of the group on either list of prioritized critical infrastructure. Third, additional lists will augment risk management and response planning. Each of the 18 sectors will have distinct lists of critical infrastructure that will determine assets and systems vital to each sector's national or regional missions. Individual states and territories may now also create specific criteria and lists of critical assets and systems. Both the new sector and state lists are for infrastructure not deemed critical enough for inclusion in the Type 1 and Type 2 lists. Thus, assets and systems that only appear on state or sector lists are not part of the two lists that include nationally critical assets or systems.

The 2009 process includes three phases: criteria development; a data call for partners to submit asset and systems and nominations of nationally critical infrastructure; and IP adjudication and reconsideration of partner list nominations. The reconsideration process grants partners the opportunity to question why IP made particular decisions regarding the exclusion of assets or systems that had been recommended for inclusion. Through reconsideration, HITRAC has shown commendable interest in ensuring that partners understand why decisions are made regarding the particular assets and systems on the lists. This should address a concern that state officials expressed to us regarding the previous process. Many states suggested to us that more information was needed on why IP made specific decisions to include to not include assets on the final lists.

IP has made other process improvements. Apart from extending timelines for information requests, IP also expanded partner involvement in sector criteria development, and made process changes to the vetting of asset and systems data.

The movement toward consequence-based criteria for nationally critical assets and systems is expected to improve the stability of the lists, which will enhance long-term risk management.

Criticality Criteria Show Improvement, With Need for More Consequence Analysis

For FY 2009, DHS moved to consequence-based criteria for the two lists of nationally critical infrastructure. This change was made in collaboration with the National Infrastructure Simulation and Analysis Center (NISAC). During our fieldwork, we compared the criticality criteria and accompanying guidance provided to partners for the FY 2006 to FY 2008 lists. Our analysis showed that sector-specific criticality criteria had been improving each year. In FY 2006, sector criteria were vague and criticality thresholds undefined. Additionally, capacity thresholds in some sectors fluctuated every year. With ongoing refinements, the criticality criteria have been better able to guide states and sectors in determining the most critical assets. DHS guidance for the process also showed improvements by increasing specificity and providing incident scenarios, specifying terms and definitions, and identifying asset and system restoration times as an element of criteria. All of this information helped partners understand what would make an asset or system rise to the level of national criticality. Ambiguous criteria make it difficult for state and sector experts to identify assets that are truly critical.

Although criteria changes have frustrated some partners, many states and sectors appreciated that DHS continues to make improvements. State representatives were encouraged by national efforts and believed that DHS is trying to close the gap of understanding through more explicit guidance. One state representative said the criteria are a “moving target” but acknowledged that the program can improve as a result. A Communications Sector expert said that DHS has “gotten better” on the creation and the revision of criticality criteria. These changes will help create the state lists and lists for each of the 18 different CIKR sectors.

Even with these improvements, understanding differences in criticality across sectors is an inherent challenge. Also, some sector and state experts said that certain criteria are difficult to measure. For example, economic loss is a criterion for various sectors, but existing models do not make it easy to assess the expected level of such loss from an attack or disruption. A dam safety expert also noted that states have various levels of expertise in completing inundation maps, tools used to predict the outcome of adverse flooding events, which is an important part of the sector's criteria.

HITRAC management said that certain criteria lacked specificity, which was a primary reason for the move toward criteria based solely on consequence in 2009. As one DHS expert noted, capacity measures such as building size, bridge length, or daily production are not necessarily appropriate measures of consequence. DHS continues to work on more specific and meaningful criteria to assist partners identify critical assets and systems.

Criticality criteria can be enhanced through an expansion of the department's consequence analysis, which examines the effect of possible terrorist attacks or natural disasters. Such work can hone existing criticality criteria and create lists that are more consistent across states and focused on assets and systems of the highest consequence. NISAC is a primary DHS entity involved in sector and cross-sector analysis. Certain sectors, states, and entities also analyze consequences of terrorist attacks or disasters.

A prominent example of NISAC's modeling work occurred prior to Hurricane Katrina. In a 41-page report, NISAC predicted that a major hurricane would cause extensive damage to New Orleans, with large numbers of casualties and extended disruption of regional and national critical infrastructure.[19] As a result of this prescient analysis, the lessons-learned report produced after Hurricane Katrina recommended that DHS expand NISAC's modeling capabilities, including further work on the economic consequence of disasters. More resources for such efforts were vital, the report noted, because governments do not have a comprehensive understanding of the interdependencies of critical infrastructure. The report stressed the continued importance of intergovernmental cooperation in modeling and consequence analysis. Specifically, DHS was asked to share all NISAC work with SSAs. Some sector experts told us that DHS can improve the amount of information that the department provides regarding NISAC's current analysis of the various infrastructure sectors.[20]

[19] "White House Got Early Warning on Katrina," *Washington Post,* January 24, 2006, p. A02.

[20] *The Federal Response to Hurricane Katrina: Lessons Learned*, February 2006, p. 61, 110-112.

Each sector's annual reports have identified ambitious modeling and consequence analysis aspirations. The Transportation Sector's report identified a need to understand how adverse events affect the transportation network, because significant work remains to identify assets and systems. According to Emergency Services Sector officials, modeling would help position resources, enhance the timeliness of first responders, and determine the effects of pandemic influenza on the sector's workforce. The identification of interdependencies through consequence analysis is a common theme in several sectors' modeling plans.

DHS recognizes the need for greater understanding of consequence. Even after the recommendation in the Katrina lessons-learned report, however, NISAC funding has been subject to debate between the executive and legislative branches. With more consistent and predictable funding, NISAC would be able to augment the DHS effort to identify critical infrastructure. Because the Science & Technology Directorate and the Federal Emergency Management Agency (FEMA) also engage in modeling, coordination with other parts of the department would be desirable. A recent National Infrastructure Advisory Council (NIAC) report recommended that new modeling efforts focus on a better understanding of sector interdependencies.[21] This sensible approach would augment the ability of DHS to see how a disruption of one sector affects others. With enhanced consequence analysis, coordinated with the SSAs, DHS would continue to improve its criteria and enhance the government's ability to identify critical infrastructure.

We recommend that the Under Secretary of the National Protection and Programs Directorate, in coordination with the Under Secretary for the Directorate of Science & Technology and the Administrator of FEMA:

Recommendation #2: Pursue and document additional budgetary resources to support necessary infrastructure modeling and consequence analysis as outlined in sectors' annual reports.

Recommendation #3: Identify and empower a single senior official to coordinate DHS modeling and consequence analysis to ensure efficient use of resources and proper sharing of plans and results with the Sector Specific Agencies.

[21] National Infrastructure Advisory Council, *Critical Infrastructure Partnership Strategic Assessment, Final Report and Recommendations*, October 14, 2008, p. 39.

Partners Provided Suggestions on Improvements to the Process

Creation of the annual lists is a complex effort, and a difficult task for several states. Some DHS partners noted that time and resource constraints can adversely affect the process. The strength of state critical infrastructure programs varies across the nation, impeding some partners' ability to provide timely and comprehensive information.

Some states and sector experts said that meeting the IP timelines is challenging. IP officials have recognized this problem, as already noted. We commend IP efforts to reduce partners' burdens. A process that takes places once every 2 years would be an additional efficiency, because states would not need to submit asset and system lists every year. According to an IP official, the lists generally do not change, and the official expects the list will be substantially similar year-to-year. An IP analyst noted that the additional time offered by a biennial, rather than annual, process would allow IP to vet the information more thoroughly. However, the Act states that the department must "maintain and annually update" the lists.[22] A biennial process is worthy of consideration, although a statutory modification would be necessary.

Most states and sector experts said DHS has improved the list process, with comments like "the process has matured" and is "getting better." Many state experts attributed improvements in the annual process to their Protective Security Advisors. PSAs serve as departmental liaisons to state, local, and tribal governments, as well as the private sector. Sectors commended IP and HITRAC staff for their willingness to work with experts outside of the department.

Partners suggested, however, that more collaboration is possible. One area of possible improvement is the provision of additional information and feedback to both states and sectors. Many states and sector experts said a lot of effort goes into responding to data calls. However, partners do not receive sufficient comments on why some assets and systems are not included on the lists or how DHS makes final list decisions. The FY 2009 process attempted to address this concern through ongoing dialogue and weekly

[22] P.L. 110-53, § 1001(c)(1).

newsletters with partners during the adjudication and reconsideration phase.

Several states indicated that DHS could help protect locally critical infrastructure and inform decisions by sharing its decisions on those assets and systems on the final lists. States would be better able to implement security measures if they know the assets and systems on the two lists of the nation's more critical infrastructure. Other state representatives saw no value in the data-intensive collection efforts. A few states further noted that more information has the potential to enhance their relationships with CIKR partners. Development of state and territory lists should increase the value of the annual process because partners can use the final lists for incident and risk management.

One way DHS can ensure collaboration is in the development of the criticality criteria. The Act requires DHS to provide the program's "data collection guidelines . . . to the appropriate homeland security official of each State." For the new consequence-based process, state officials nominate assets based on their own criteria development process. This allows states to explain why particular assets are nominated as critical infrastructure. IP still uses national criticality criteria for the sectors to determine the assets or systems that will make the final lists.

Historically, a limited number of states had an opportunity to review and provide comments on the national criteria through the State, Local, Tribal and Territorial Government Coordinating Council. Officials from only 15 states and two tribal jurisdictions were represented on this council. Some officials in the 15 states were at the local level and cannot speak for the state as a whole. Additionally, larger states like Illinois, Ohio, Pennsylvania, and Texas are not represented.

The states and the SSAs rely on the private sector for information on assets and systems that meet the criteria. With the exception of a few regulated sectors, such as the Banking and Finance, Chemical, and Nuclear sectors, the private sector voluntarily provides information to the government. According to states and sector experts, some private sector partners do not understand the value of sharing information because the benefits of the annual list process are not evident. The private sector views timely information on specific CIKR threats as necessary, but the needed communication does not always take place. Several private sector experts provide information to DHS, but they do not receive the final lists.

Several factors hamper DHS' ability to share information with its CIKR partners. Although information submitted by states and sector experts is unclassified, the final lists are classified Secret. This presents an obstacle to stakeholders who do not have the necessary clearance. Threat information from intelligence agencies is also classified, which can be an impediment to information sharing. NIAC noted similar problems in a cyber security report. The intelligence on cyber threats to critical infrastructure control systems is not often shared with the owners of those systems. To address the obstacles faced by CIKR owners and operators, NIAC made several recommendations.[23]

In a previous report, we noted the gap between stakeholder expectations and DHS capabilities and programs in the sharing of classified information.[24] To provide value to partners, DHS should enhance its ability to share the final lists and strategic threat information concerning the nation's critical assets and systems with the private sector.

We recommend that the Assistant Secretary for the Office of Infrastructure Protection:

Recommendation #4: Ensure that all states are allowed to review the criticality criteria on an annual basis.

Recommendation #5: Develop policies that would lead to greater sharing of final lists with partners and provide specific guidance to partners on sharing sensitive and classified information.

Sectors Have Varying Levels of Concern About Cyber Infrastructure

Electronic information and control systems are a central element of many infrastructure sectors. These cyber systems direct essential CIKR processes and functions. The NIPP defines cyber security as

[23] The National Infrastructure Advisory Council Convergence of Physical and Cyber Technologies and Related Security Management Challenges Working Group, *Final Report and Recommendations by the Council*, pp. 25–27.

[24] DHS OIG, *Challenges Remain in Securing the Nation's Cyber Infrastructure*, OIG-07-48, June 2007, p. 17.

> *The prevention of damage to, unauthorized use of, or exploitation of, and if needed, the restoration of electronic information and communications systems and the information contained therein to assure confidentiality, integrity, and availability.*[25]

The NIPP concluded that the U.S. economy and national security are highly dependent upon global cyber infrastructure, which has created an interconnected and interdependent global network. The NIPP noted that this level of interdependence created a linkage between physical and cyber elements of CIKR.

National progress has been made in securing the cyber component of critical infrastructure operations. In a January 2007 report, NIAC identified a dedicated community of individuals and programs working to protect control systems for critical infrastructure sectors. These "strong and committed governmental efforts" are highly valuable to several sectors.[26] The National Cyber Security Division in NPPD is charged with reducing cyber risk across the sectors. One of the division's two strategic objectives is to implement a cyber risk management program for protection of critical infrastructure.

NPPD has a wide range of cyber risk mitigation responsibilities, including national threat assessments, cross-sector analysis, and coordination of security programs. SSAs add expertise to ensure that security strategies and protective activities include fully integrated cyber perspectives. According to the NIPP, DHS databases and cataloging efforts should include appropriate information on sectors' cyber assets, systems, networks, and functions. Existing documents, such as cyber roadmaps for electrical and water utilities, help infrastructure operators understand the nature of the cyber threat.

The NIPP notes that "cyber interdependence presents a unique challenge for all sectors."[27] Thus, like overall CIKR identification, cross-sector cyber work is inherently difficult. In our discussions with public and private experts across 15 sectors, most noted the importance of cyber security. However, many experts said that

[25] DHS, *National Infrastructure Protection Plan*, p. 109.

[26] National Infrastructure Advisory Council Convergence of Physical and Cyber Technologies and Related Security Management Challenges Working Group, *Final Report and Recommendations by the Council*, p. 5.

[27] DHS, *National Infrastructure Protection Plan*, p. 35.

more pressing concerns, such as attacks on buildings or the possibility of biological contamination, are a higher priority. A security manager for one non-DHS SSA said that the sector has no cyber security concerns, while others believed that attacks on asset control systems would not create nationally significant problems. Some state experts suggested that staffing limitations or the need for more expertise hinders their cyber asset identification.

These issues may explain why most sectors have a limited emphasis on cyber criticality criteria. A criterion for the Freight Rail subsector suggests that states submit cyber systems that would create a loss of signaling apparatus and disrupt the monitoring of rail cars in transit. A freight rail expert told us that cyber issues are vital to the market viability of railroad companies. Cyber disruption could have devastating economic consequences. In line with the sector's criteria, some freight rail signaling stations were submitted for the 2008 process.

Specific cyber identification criteria for each sector would likely not improve cyber security overall. Many assets with cyber components are already identified on the lists without itemizing cyber systems or interdependencies. Sectors with greater concern about cyber security did note positive work with HITRAC on cyber assets, and some regulatory entities, such as the Nuclear Regulatory Commission, help focus asset owners on enhancing cyber security. As DHS expands its risk analysis and understanding of cross-sector dependencies, the need for specific cyber criteria for various sectors may appear.

Some "Systems-Based" Sectors Have Problems Identifying Critical Components

Existing law defines critical infrastructure as "systems and assets" vital to the United States.[28] Infrastructure sectors that include buildings and structures, such as chemical plants and nuclear reactors, are considered asset-based. These sectors rely on supply chains and inter-sector linkages but are centered on a single facility. Conversely, sectors that have intangible assets or that work across a range of facilities are systems-based. Systems-based sectors have had varying levels of success with the process to identify nationally critical infrastructure.

DHS defines a system as:[29]

> "Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose."

Individual assets in a systems-based sector, such as a bank or food-processing facility, are generally not seen as individually critical. Table 2 provides examples of both asset- and systems-based sectors.

Table 2. Certain asset- and systems-based sectors

Asset-based sectors	Systems-based sectors
Chemical	Agriculture and Food
Commercial Facilities	Banking and Finance
Dams	Communications
Defense Industrial Base	Energy
Nuclear	Information Technology

Experts suggested that other sectors, such as Emergency Services and Water, are also systems based. Others can be considered critical from both asset and systems perspectives. According to the Transportation Sector Specific Plan, for example, transit modes can be collectively evaluated as a system. Nonetheless, the sector has placed great emphasis on protecting certain assets, such as subway stations.

[28] 42 U.S.C. § 5195c(e).

[29] DHS, *National Infrastructure Protection Plan*, p. 111.

Identifying and protecting fixed assets is not as difficult as defining critical systems. Thus, DHS efforts to categorize critical infrastructure have focused on assets. Since our 2007 food defense report, DHS has made some progress in identifying systems, including the study of vulnerabilities in interdependent sectors.[30] Even sectors that have experienced frustration in this area have noted the department's commitment to find mutually agreeable solutions. However, systems identification problems are still evident, leading to frustration in certain sectors and the potential for some disruption of DHS infrastructure partnerships.

Several of the officials we interviewed noted the difficulty in identifying systems for the lists, with one official declaring that DHS "ignores history" by being more concerned with fixed sites than supply chains. PSAs also told us that more work in the systems area is needed. Of the 59 PSAs providing an opinion, only 12 believed that the current effort to identify systems ranked as a 4 or 5 on a five-point scale, while 26 PSAs rated the effort as poor or below average. PSAs commenting on the identification of systems noted:

> "I strongly believe we need to do a better job in the systems based sectors (especially the agriculture sector)."

> "Systems based sectors are [the] weakest part of the lists."

> "A systems approach needs to be adopted . . . systems interdependencies may well become our national weakness, rather than any individual, or set of stand-alone sites."

During our fieldwork, we encountered a range of opinions regarding the success of integrating the systems concept into critical infrastructure protection and asset identification. The Emergency Services Sector noted the difficulty of establishing a systems view of its components. The Transportation Security Administration (TSA) was pleased that IP recognized the systems-based nature of important transit elements, such as rail systems. List submissions for large subways are based on one overall system, rather than individual stations. Neither TSA nor the states

[30] DHS OIG, *The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection*, OIG-07-33, March 2007.

submit station stops for subway systems. Although individual stations have been targeted in terrorist attacks, TSA experts noted that any point of an overall rail system could be infiltrated, making large transit systems, not stations themselves, nationally critical. TSA appreciates the flexibility that has led to the submission of individual rail systems for the lists. Our 2006 report on the NADB identified inconsistencies in state transit rail data submissions. For example, some states provided the name of one rail system, while others submitted lists of all stations. Cooperation between TSA and IP has ended this problem, ensuring more consistency across the nation's transit rail systems and other components of the Transportation Sector.

Of the sectors that continue to struggle with systems identification, the most difficult case has been the Agriculture and Food Sector. Our March 2007 food defense report documented the sector's concern regarding the identification of systems. The experts we interviewed for this report said that the annual process continues to leave the sector with a much smaller number of assets than other sectors. These conclusions were noted in the sector's July 2007 annual report. The department's 2008 list guidance for the sector still advised state agencies to identify only assets that, if damaged, destroyed, or compromised, could create the highest consequences on a regional or national scale. This guidance minimized systems identification.

There is some merit to the department's approach. Although one cow with hoof-and-mouth disease could create nationally significant problems, one animal cannot be seen as nationally critical. DHS prefers that states identify specific parts of diverse interstate food production systems and other sector subcomponents that meet the criticality criteria. HITRAC and sector experts share the view that identifying critical portions of the Agriculture and Food Sector is a major challenge. Experts we interviewed from the sector noted that DHS is interested in exploring solutions to this difficult problem. The critical clusters approach in the 2009 process can be seen as one way to expand systems identification.

Since our 2007 food defense report, the National Center for Food Protection and Defense created a new identification method. The Food and Agriculture Sector Criticality Assessment Tool (FASCAT) was developed in consultation with sector experts and has the support of DHS and the sector's two SSAs. IP officials have noted that states using FASCAT may leverage information gathered through that effort. Nonetheless, the SSAs believe the

2008 list process was difficult, which created “a mixed bag” of state submissions.

After receiving more than 1,600 Agriculture and Food Sector submissions from 34 states and territories, DHS asked the SSAs to reduce the list. Even after the list decreased significantly, DHS did not accept the submissions for the nationally critical lists. SSA staff said that DHS was concerned about consistency across states and the level of assets submitted that did not meet the sector’s general criteria.

Some states and territories submitted hundreds of items, while 22 states and territories did not provide any Agriculture and Food Sector assets or systems. The SSAs have legitimate concerns that the result of the 2009 process will hamper state interest in providing food and agriculture assets and systems, if not severely harm the sector’s partnership model. No portion of the sector’s production and processing system, a highly significant part of the U.S. economy and a net exporter, appears on a list of nationally significant critical infrastructure. This is especially difficult to understand when the sector’s regulatory bodies hold such extensive data about the sector.

We acknowledge that systems identification is complicated. However, DHS should work with the SSAs and the sector’s coordinating councils to create general criteria based on state production capacity and the value of food produced. The current criteria focus on public health or economic loss from intentional or natural disruptions, criteria that are difficult for states to predict. Although state production criteria would lack vigorous consequence and vulnerability components, the criteria could be enhanced through modeling efforts and further refinement. Moreover, SSA submission of data would end the problem of inconsistency across states and reduce the states’ burden. For example, SSAs can easily determine which states produce the most milk, beef, and other popular commodities. Using the lists to catalog the sector’s most productive subcomponents is necessary for the Agriculture and Food Sector to be suitably represented compared to other sectors.

We recommend that the Assistant Secretary for the Office of Infrastructure Protection:

Recommendation #6: Create criticality criteria based on existing state production and capacity data, which would lead the Sector

Specific Agencies, rather than the states, to submit data for the lists.

Protective Security Advisors Displayed Some Confusion About Their Role

The annual list process has helped DHS and its partners to improve critical infrastructure protection through the identification of nationally critical assets. We initiated a survey of PSAs, DHS employees in the field who work with states and sectors. These experienced professionals are an important part of CIKR protection. Many PSAs believe that DHS has taken positive actions to protect CIKR. Nonetheless, some PSAs expressed a degree of negativity about IP's CIKR protective efforts. Based on PSA comments, we did not conclude that the lists are seriously flawed, but the comments justify further DHS focus on the role of the PSAs in working with partners to develop the lists.

Some PSAs noted that industry experts have created CIKR asset lists. According to some PSAs, these lists had key differences from the lists of nationally critical infrastructure. Several PSAs wrote that the criteria, although improving each year, need further refinement. One PSA suggested that IP should ensure that PSAs do more to coordinate with states on establishing submission parameters, while another suggested mandated coordination between PSAs and the public and private sector partners that submit data.

Most of the PSAs who answered the question, 53 of 61 (87%), advocated for some private sector involvement in the list process. Such an enhancement could improve the accuracy of list submissions.

Only a small majority, 33 of 61 (54%), believed that PSAs should be more involved in the process. Yet, PSAs were generally displeased with their ability to influence CIKR policies and practices. PSAs commented that more work is needed to improve states' submissions and facilitate greater interaction with SSAs. Several noted the difficulty of explaining DHS decisions to the states, especially when assets submitted by states are not on the final lists.

Although IP has shown continued interest in revising the process used to identify nationally critical infrastructure, further work to refine the PSA role is warranted. Specific steps in this area should focus on ensuring that PSAs participate in state list submissions, as well as on further coordination between PSAs and SSAs. All of the state officials we interviewed praised the work of individual PSAs and considered them an invaluable resource. Additional work in this area would improve asset identification and the ability of DHS to work with security partners.

We recommend that the Assistant Secretary for the Office of Infrastructure Protection:

Recommendation #7: Expand the role of Protective Security Advisors in the annual list process to enable them to provide information and comments on state data submissions.

The Lists are Used in Grant Formulas, but Not by DHS Law Enforcement

The Lists Are Used in the Allocation of Grant Funding

The nation must prioritize its grant funding and protective efforts to target areas most in need. Data gained through the two lists of nationally critical infrastructure are provided to FEMA for use in two parts of the Homeland Security Grant Program: The State Homeland Security Program (SHSP) and the Urban Areas Security Initiative (UASI). In FY 2008, all 50 states, the District of Columbia, and five territories were eligible for $861,280,000 in SHSP funding. Also in FY 2008, $781,630,000 was available under the UASI for the nation's 60 most at risk urban areas. The new sector and state lists of critical infrastructure are not used for purposes of grant funding.

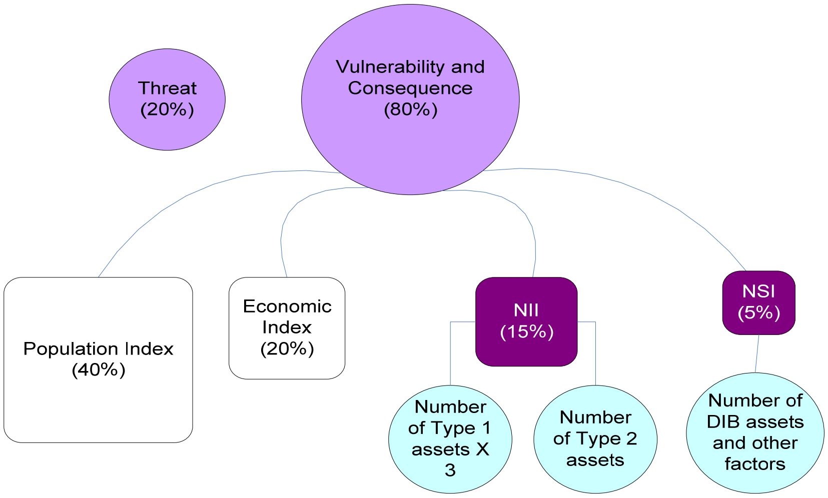
The SHSP and UASI funding formula is based on the department's definition of risk, which includes three elements: threat, vulnerability, and consequence.[31] Intelligence analysis is used to create the threat component of the formula, which accounts for 20% of the allocations for the two programs. The vulnerability and consequence portions account for the remaining 80%.

Four indices compose the formula's vulnerability and consequence elements, or 80% of the overall allocations. A Population Index accounts for 40% of vulnerability and consequence, while an Economic Index accounts for 20%. The National Infrastructure

[31] DHS, *National Infrastructure Protection Plan*, p. 32.

Index (NII) and the National Security Index (NSI) account for the remaining 20% of the formula's vulnerability and consequence portion. FEMA uses list statistics to create the NII and the NSI. The NII, which uses a jurisdiction's number of nationally critical assets, is 15% of the vulnerability and consequence total. The NSI, which includes the number of nationally critical assets in the Defense Industrial Base (DIB) Sector as one component, is 5%.[32] Figure 1 illustrates the placement of list data in the risk formula.

Figure 1. Nationally Critical Asset Information and the SHSP and UASI formula


Threat (20%)
Vulnerability and Consequence (80%)
Population Index (40%)
Economic Index (20%)
NII (15%)
NSI (5%)
Number of Type 1 assets X 3
Number of Type 2 assets
Number of DIB assets and other factors

States are required to send 80% of total SHSP and UASI funding to local governments. Guidance for the 2009 grant programs included six Homeland Security Grant Program national priorities that were to inform state applications:

- Progress in meeting the National Preparedness Guidelines
- Protecting against improvised explosive devices
- Strengthening preparedness planning, training, and exercises
- Emphasizing information-sharing capabilities
- Strengthening medical readiness
- Strengthening preventive radiological/nuclear detection capabilities

Although these guidelines relate to critical infrastructure protection, the SHSP is designed to help develop state and local preparedness

[32] GAO, *Homeland Security: DHS Risk-Based Grant Methodology Is Reasonable, But Current Version's Measure of Vulnerability is Limited*, GAO-08-852, June 2008.

and response capabilities. UASI funds focus on regional protection of the nation's larger urban areas. A focus on improvised explosive devices came from Homeland Security Presidential Directive 19, "Combating Terrorist Use of Explosives in the United States."

Grants Using Nationally Critical Asset Data Do Not Require Direct Expenditures to Protect Those Assets

SHSP and UASI are designed to improve state and territorial capacity to protect the nation and respond to major events. The NIPP establishes that SHSP and UASI funding should address:

> "*regionally or locally critical priority CIKR initiatives. A further prioritized combination of grant funding across various programs may be necessary to enable the protection of certain assets, systems, networks, and functions deemed to be nationally critical.*"[33]

This language does not preclude the use of SHSP and UASI funding to protect nationally critical infrastructure. Sending funding to states based on the existence of nationally significant CIKR does not mean that states will use that funding to protect or aid response and recovery efforts for those assets. However, current law establishes that states may use allocations from the two programs for various purposes, including protecting a nationally critical system or asset.[34] Although national criticality need not influence all state allocation decisions, federal funds are being used to augment state goals. Funding that is partially based on two lists of nationally critical infrastructure allows state and local officials to make provincial decisions about how to allocate funds. The number of nationally critical assets in a jurisdiction may or may not be a good proxy for the amount of money needed for regionally or locally critical priority CIKR initiatives. Although risk management theory suggests that funds should "buy down" risk, experts do not know how UASI and SHSP grant allocations are decreasing overall risk or improving the protected status of nationally critical infrastructure.[35]

The FEMA officials we interviewed said that states must provide investment justifications for allocated funding. Additionally, a peer review of state submissions is designed to ensure that state

[33] DHS, *National Infrastructure Protection Plan*, p. 102.
[34] 6 U.S.C. § 609(a)(3).
[35] RAND, "Estimating Terrorism Risk," 2005.

funding corresponds with national or state goals. FEMA is developing a cost-to-capabilities initiative to measure how grant funding leads to security improvements. This information will be used to target programs, fill security gaps, and connect funding to DHS policy. These efforts have merit. However, existing rules allow the spending of national SHSP and UASI funds based on state interests. Although DHS guidelines help in funding decisions, states may have a different view of risk than the department.

Security improvements to critical assets are part of certain other grant programs. For FY 2008, DHS provided states $48,575,000 in Buffer Zone funding for list assets.[36] The equipment needed for protection and resiliency is vetted against an authorized equipment list, to ensure the grant money is used appropriately to mitigate security gaps identified in the Buffer Zone Plans. After the vetting process, DHS releases the funds. Additionally, a focus on improvised explosive device prevention clearly has protective value for critical infrastructure sites. However, guidance from FEMA stated that grant allocations to protect against these devices "should be undertaken in coordination with the statewide CIKR protection program," which could target assets that are not nationally critical.

Under Homeland Security Presidential Directive 8, preparedness grants are not designed "to support existing capacity to address normal local first responder operations, but to build capacity to address major events, especially terrorism."[37] Some state officials noted that some jurisdictions were using funding for ongoing local concerns. Direct correlation between UASI and SHSP funding and nationally significant assets and systems would ensure greater linkage between grant funding and national goals.

Although the number of assets placed on the lists affects a state's grant funding, data are not readily available to show how states use UASI and SHSP funding to protect CIKR sites. The need for such spending data has created frustration in SSAs that have infrastructure protection programs. Agency experts informed us that inefficiencies and duplication of agencies' efforts are occurring.

[36] DHS, *Overview: FY 2008 Infrastructure Protection Activities*, May 2008, pp. 5, 20–21.

[37] Homeland Security Presidential Directive 8, December 13, 2003, paragraph 11.

Officials from the Nuclear and Water Sectors expressed the most irritation about the need for data on grant funding decisions. Environmental Protection Agency experts considered it embarrassing that federal partners may be allocating security funding to the same projects. Security staff at the Nuclear Regulatory Commission said that sectors cannot see “a connection to a purchase” after states allocate DHS grant dollars. This hampers the government’s ability to learn how security gaps are being lessened through allocation of federal funds. The Nuclear Regulatory Commission noted that because states spend SHSP and UASI funds, the federal government would not have data to share with the SSAs regarding spending decisions. Although DHS has conducted some information sharing in this area, concern about a need for dialog was not limited to federal agencies. Some state interviewees lamented the incomplete dialog with SSAs on grant funding issues.

Without better data on SHSP and UASI funding, a complete assessment of risk reduction will be elusive. An expert risk management forum noted that the government must “be able to estimate the level of deterrence resulting from the countermeasures implemented.”[38] Constraints on this front led sector experts to complain that even though asset data affects grant funding, “whiz-bang” devices purchased throughout the country have limited utility in national risk reduction. Another expert opined that grant funding efforts cannot be deemed a success simply by counting the number of new fire trucks.

Response and recovery are logical places for SHSP and UASI allocations. A new objective to link funds to assets and systems on the lists would better protect the nation’s most critical infrastructure. FEMA should work with NPPD to develop a grant objective that establishes a link between grant funds and list entries. To address the concern about incomplete grant information sharing, FEMA could collect data from the states on funds that were spent on particular sectors, and share the data with the SSAs. Improved interaction between SSAs and states would decrease the potential duplication of effort and provide information on what sectors are receiving funding. With knowledge about how sectors are using UASI and SHSP funding, DHS would be better able to target protective efforts on nationally critical infrastructure.

[38] GAO, *Highlights of a GAO Forum: Strengthening the Use of Risk Management Principles in Homeland Security*, GAO-08-627SP, April 2008, p. 13.

We recommend that the Administrator of FEMA, in coordination with the Assistant Secretary for the Office of Infrastructure Protection:

Recommendation #8: Create an objective in annual grant guidance that links a portion of State Homeland Security Program and Urban Area Security Initiative funding to the protection of nationally critical assets and systems.

Recommendation #9: Collect and disseminate grant expenditure data that inform Sector Specific Agencies about the amount of funds that states spend on particular sectors' assets and systems.

The Lists are Not Meant to Assist Law Enforcement Efforts

DHS agencies are charged with enforcing a variety of U.S. laws. Immigration and Customs Enforcement (ICE) conducts operations against employers who hire undocumented workers. In FY 2008, ICE made 6,287 criminal and administrative arrests as a result of worksite enforcement operations. ICE intends to target critical infrastructure sites that may employ individuals who are not authorized to work in the United States. Although ICE lists airports, nuclear power plants, and chemical facilities as examples of critical infrastructure, ICE and IP do not have sufficient ongoing contact to help both entities achieve mutual CIKR protection goals.

An ICE manager who deals with worksite enforcement investigations noted that ICE would like to target investigative resources on facilities deemed most vital, but ICE does not have access to current lists. ICE management noted that the agency does not interact with IP on specific CIKR sites or general areas of shared interest.

HITRAC officials noted that the list process is not focused on aiding law enforcement. They believe that use of the lists for law enforcement purposes, especially actions as sensitive as immigration worksite operations, would seriously hinder the overall partnership model. HITRAC believes that some states and the private sector would be reluctant to participate in the process if it were used for immigration enforcement operations. Very clear rules would be required to denote the limits of information sharing if DHS agencies were to use the lists for investigative or other purposes. Nonetheless, HITRAC officials are not opposed to collaborating with ICE on matters of critical infrastructure protection. We believe that such collaboration would be beneficial to both HITRAC and ICE.

IP has concerns about the use of the nationally critical lists for DHS law enforcement work. Nonetheless, an enhanced partnership offers ICE and IP the ability to augment DHS critical infrastructure protection objectives. Although we are not recommending that the lists be shared with DHS law enforcement agencies, an expanded dialog could offer mutual benefits for IP and ICE.

We recommend that the Assistant Secretary for the Office of Infrastructure Protection:

Recommendation #10: Confer with Immigration and Customs Enforcement on the mutual goal of protecting critical infrastructure and report to the Office of Inspector General on methods and remaining obstacles to intra-departmental coordination and information sharing on critical infrastructure protection.

Status of DHS Reporting Requirements and Discretionary Consortium

The Act requires that DHS submit a report on efforts to identify and catalog critical infrastructure.[39] In its report, IP explained that the IDW will house the nation's infrastructure data. As required by the Act, IP also provided a synopsis of significant challenges associated with the database and the annual process to identify nationally critical infrastructure.

The Act included discretionary language allowing DHS to establish a National Infrastructure Protection Consortium to advise "on the best way to identify, generate, organize, and maintain any database or list of systems and assets."[40] In addition to government experts, this group could include national laboratories, academic institutions, or Centers of Excellence, which are groups of experts that work with the department to address various homeland security issues. A few sector experts expressed interest in an additional entity to identify critical infrastructure asset and systems. However, most believed that the current NIPP sector partnership model would be more suitable to handle critical infrastructure asset and system identification activities.

[39] P.L. 110-53, § 1001(d).
[40] P.L. 110-53, § 1001(f).

Partners said that the existing model has made progress in building relationships and trust between the government and the private sector. One PSA said that the "relationships and processes are in place and becoming more effective each year." Other sector partners argued that an additional commission would be redundant. PSAs were divided on establishing the Consortium, 31 suggested its adoption while 30 were opposed.

Major Changes to the Sector Partnership Model Are Not Needed

Experts who had concerns about some DHS policies and actions have noted ongoing improvement in their work with the department. DHS continues to search for ways to improve the partnership model. Further improvements can be made, but we are pleased that infrastructure sectors have seen a growing DHS commitment. Major changes to the sector partnership model are not necessary. Revisions to the model must respect the advancements DHS has made. Through our continuing examination of DHS work with other sectors, departmental acquisition practices, and related areas, we will continue to evaluate efforts to identify and protect critical infrastructure, a vital component of the DHS mission.

Management Comments and OIG Analysis

DHS consolidated responses from NPPD, FEMA, and ICE to provide written comments on our draft report. We evaluated the comments and have made changes where we deemed appropriate. DHS concurred with 8 of 10 recommendations. Below is a summary of the consolidated comments and our analysis. The department's response is included as Appendix B.

Recommendation #1: Complete the acquisition process for the Infrastructure Information Collection System.

Management Comments to Recommendation #1

The department concurred with our recommendation. IP will continue to work with the Under Secretary for Management to acquire the Infrastructure Information Collection System. The system is viewed as an improved approach to collecting and maintaining reliable information on the nation's infrastructure.

OIG Analysis

We consider the department's reply responsive to the recommendation. We will require updates on the IICS acquisition efforts. This information should include challenges faced in completing the acquisition. The recommendation is *resolved and open.*

Recommendation #2: Pursue and document additional budgetary resources to support necessary infrastructure modeling and consequence analysis as outlined in sectors' annual reports.

Management Comments to Recommendation #2

The department concurred with our recommendation. Current funding levels allow DHS only to support HITRAC requests and the maintenance of existing NISAC capabilities, although DHS sees the need for expanded capabilities to fully serve the NIPP partnership model. A necessary first step before pursuing additional resources will be to identify the universe of consequence analysis needs across DHS.

OIG Analysis

We consider the department's reply responsive to the recommendation. The single DHS contact assigned under Recommendation #3 should ensure coordination of the effort to acquire additional consequence analysis resources across various agencies. Expansion of the department's capabilities in this area is central to improving analysis of interdependencies across the 18 critical infrastructure sectors. We will require updates on the department's efforts to identify its scope of capability in infrastructure modeling and consequence analysis and the resulting actions to document resources dedicated to such efforts. This recommendation remains *resolved and open*.

Recommendation #3: Identify and empower a single senior official to coordinate DHS modeling and consequence analysis to ensure efficient use of resources and proper sharing of plans and results with the Sector Specific Agencies.

Management Comments to Recommendation #3

DHS concurred with our recommendation. The response focused on a need for coordination between a range of components. This would ensure that a department-wide perspective, not just that of any one component, will drive national modeling and consequence analysis. An Executive Steering Committee, composed of various DHS stakeholders, would ensure the necessary coordination. Such an entity would capture the perspective of various DHS stakeholders.

OIG Analysis

We consider the department's reply responsive to the recommendation. DHS has commendable plans in this area. Input of various DHS components will be necessary to bring maximum efficiency to this important effort. When fully coordinated, modeling and consequence analysis will improve DHS efforts to identify each sector's most critical infrastructure. The Executive Steering Committee should bring an important inter-component view to this effort. We will require updates on the department's plans as outlined in its response. This recommendation remains *resolved and open*.

Recommendation #4: Ensure that all states are allowed to review the criticality criteria on an annual basis.

Management Comments to Recommendation #4

The department concurred, noting that the FY 2009 process addresses our recommendation. Revisions to the process for FY 2009 granted states an opportunity to comment on the existing consequence-based criteria. Also, states and territories are able to develop unique criticality criteria for lists of critical infrastructure in their jurisdictions.

OIG Analysis

IP actions for the FY 2009 process are responsive to the recommendation. Because the intent of state involvement in annual criteria found in the *Implementing Recommendations of the 9/11 Commission Act of 2007* has been addressed, we consider this recommendation *resolved and closed.* No further action is required.

Recommendation #5: Develop policies that would lead to greater sharing of final lists with partners and provide specific guidance to partners on sharing sensitive and classified information.

Management Comments to Recommendation #5

The department concurred with our recommendation.

OIG Analysis

While the department has concurred, there was no indication in its response on what actions will be taken to address this recommendation. We understand that PSAs and other DHS staff continue to work with states on sharing sensitive information. This recommendation will remain *resolved and open* until the department provides further information on how it will address greater sharing of lists.

Recommendation #6: Create criticality criteria based on existing state production and capacity data, which would lead the Sector Specific Agencies, rather than the states, to submit data for the lists.

Management Comments to Recommendation #6

The department did not concur with this recommendation. Use of federal agencies' capacity data is seen as a step back from the consequence-based focus that is now used to identify the critical assets and systems. FASCAT, adopted through a collaborative process with the sector, will continue to guide identification efforts. DHS argued that states are the best entities to identify the sector's most critical assets and systems.

OIG Analysis

The department's response is true to the intent of our recommendation, which was based on a concern about the Food and Agriculture Sector's inability to be represented in the annual list process. Use of capacity data was one way to rectify this problem. Although FASCAT has support from sector experts, the 2008 process did not satisfy the sector's two SSAs. Nonetheless, IP's focus on continually improving the systems identification effort is a positive sign. If fully developed to its potential, FASCAT can lead to greater sector representation on the lists. Thus, we consider this recommendation *resolved and open,* pending data and further updates on progress made to integrate the sector's most critical systems into the process.

Recommendation #7: Expand the role of Protective Security Advisors in the annual list process to enable them to provide information and comments on state data submissions.

Management Comments to Recommendation #7

DHS concurred with our recommendation to expand the PSA role in the process.

OIG Analysis

The department concurred with our recommendation, but no additional detail was provided beyond noting that PSA involvement was expanded in FY 2009. HITRAC FY 2009 guidance notes a role for PSAs in nominating submissions for the Emergency Services Sector. However, there is no indication of further PSA roles in the guidance. Additional information is needed on how the PSA role has been expanded. This recommendation is *resolved and open*.

Recommendation #8: Create an objective in annual grant guidance that links a portion of State Homeland Security Program and Urban Area Security Initiative funding to the protection of nationally critical assets and systems.

Management Comments to Recommendation #8

The department did not concur with our recommendation. DHS argued that the Buffer Zone Protection Program fulfills the linkage our recommendation envisions. In its response, the department noted that BZPP provides $50 million annually to local law enforcement and public safety agencies to address CIKR security gaps for nationally critical assets.

OIG Analysis

We reaffirm our recommendation. While BZPP grants are designed to increase the protection of nationally critical assets and systems, the funding available for this program has been significantly less than funds disbursed for SHSP and UASI grants. In FY 2008 alone, DHS provided over $861 million SHSP and $781 million UASI funds to states.

FEMA's strategic plan indicates that grants are important resources to influence actions and develop integrated and comprehensive capabilities that will achieve national objectives. The agency specifically notes that it will promote the protection of critical infrastructure to avoid major disruption to commerce or significant loss of life. FEMA will also work to ensure that "capabilities for all hazards are strengthened and based soundly on a joint analysis of risk . . ." Focusing funding on nationally critical assets and systems, rather than infrastructure deemed important just at the state level, most obviously fits into FEMA's critical infrastructure protection goals. Because the process identifies the most nationally critical infrastructure, grant programs receiving funds partially based on list entries should include an objective to protect these assets.

Protection of assets identified on the lists is the best way to maximize investments.

Recognizing that not all assets and systems are equally important across the 18 sectors, DHS expends a great deal of effort annually to identify nationally critical assets. DHS grants are an important tool used to focus federal resources on the nation's highest CIKR priorities. Since a portion of SHSP and UASI grants is calculated using list data, a portion of the funds should be directly linked to the protection of nationally critical assets and systems. Some funds may still be used for states to protect assets and systems that are critical only on the local level. Our recommendation seeks to establish the linkage between a portion of SHSP and UASI funding to protection of nationally critical assets and systems through an objective in grant guidelines. Other approaches could meet the intent of our recommendation, such as channeling the portions of SHSP and UASI funds directly tied to the lists to grant programs like the BZPP. This recommendation remains *unresolved and open*.

Recommendation #9: Collect and disseminate grant expenditure data that inform Sector Specific Agencies about the amount of funds that states spend on particular sectors' assets and systems.

Management Comments to Recommendation #9

The department concurred with our recommendation. Through consultations with IP, FEMA will determine how grant reporting systems can be used to inform SSAs on how funding has been used at the state and local level.

OIG Analysis

We consider the department's reply responsive to the recommendation. Once data is gathered DHS will be able to determine the level of state funding tied directly to national goals, which is in line with FEMA's strategic plan. This will also help DHS work with SSAs to avoid duplicate security spending. We will require updates regarding the results of the FEMA-IP discussions on reporting states' grant expenditures to the Sector Specific Agencies. This recommendation is *resolved and open*.

Recommendation #10: Confer with Immigration and Customs Enforcement on the mutual goal of protecting critical infrastructure and report to the Office of Inspector General on methods and remaining obstacles to intra-departmental coordination and information sharing on critical infrastructure protection.

Management Comments to Recommendation #10

The department concurred with our recommendation. Outside of the formal comment process, some concern still exists regarding the potential impact of sharing list entries with law enforcement.

OIG Analysis

We consider the department's reply responsive to the recommendation. As stated in our report, the recommendation was based on the need for greater consultation between IP and ICE. This interaction does not require that IP share the lists with ICE or other law enforcement entities. We will require reports on the results of NPPD discussions with ICE regarding methods and remaining obstacles to intra-departmental coordination and information sharing on critical infrastructure protection. This recommendation is *resolved and open*.

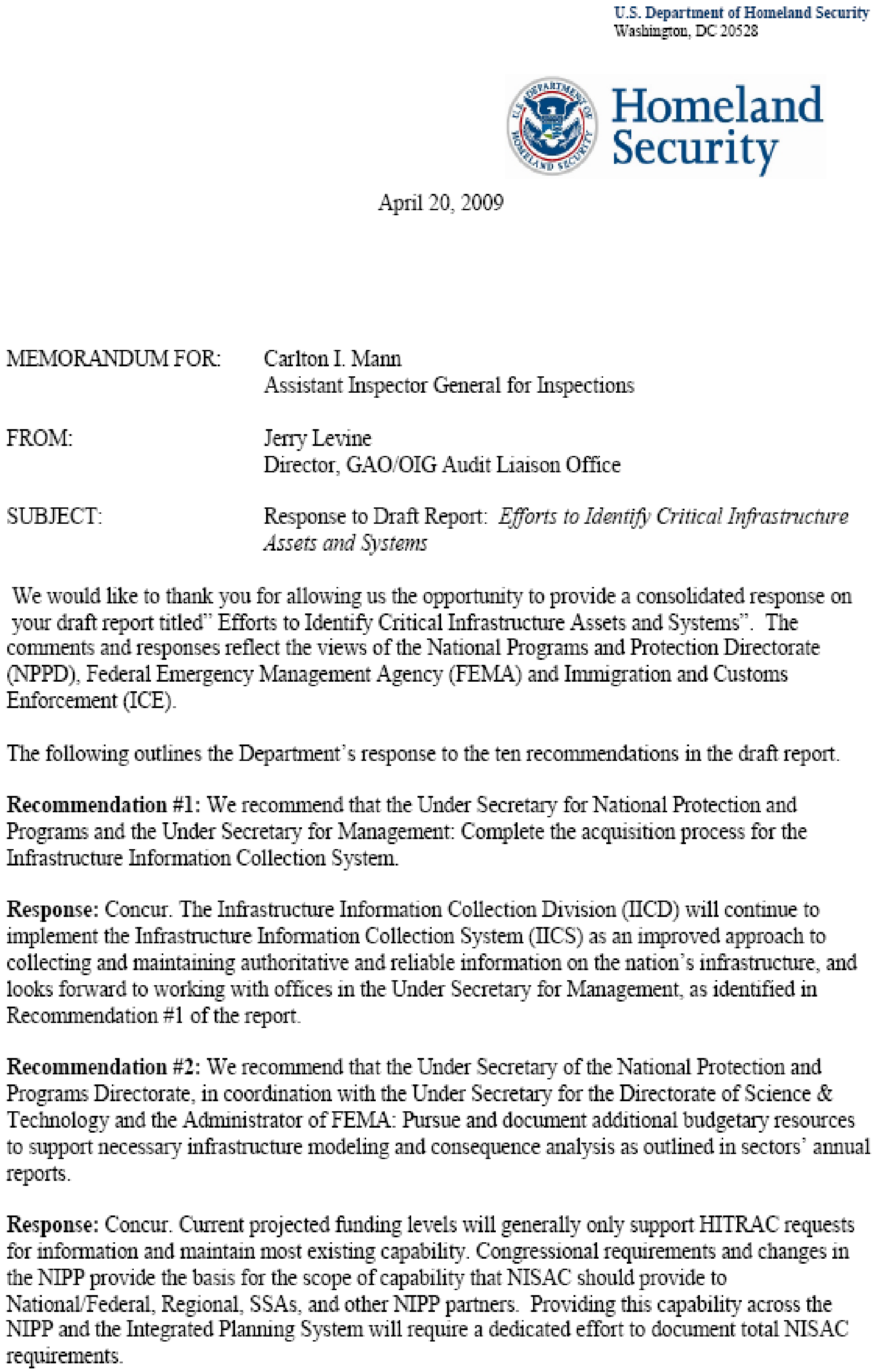
Section 1001 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53) required our office to review how DHS identifies and catalogs the nation's critical infrastructure. We examined a wide range of general information about each of the critical infrastructure sectors. We reviewed statutes and policies related to CIKR protection, as well as risk management documents. We did not evaluate the exact points where problems in NPPD or the Directorate of Management adversely affected the development of the IICS.

We conducted 53 interviews, including discussions with 15 state homeland security offices and 31 experts representing 15 of the 18 infrastructure sectors. We interviewed DHS branch chiefs, members of the Government and Sector Coordinating Councils, and other individuals with expertise in critical infrastructure protection policy. Additionally, we attended the 2008 Critical Infrastructure Protection Congress.

To gain the perspective of PSAs, we created an online survey that was distributed to 75 PSAs. We received 63 responses, a response rate of 84%. Fifty-one of the 63 respondents, or 81%, had been PSAs for more than 2 years. Survey questions dealt with PSA perspectives on asset identification work and the overall risk management process. Results of the survey are discussed throughout the report; the survey appears in Appendix C.

We conducted our review between July and October 2008 under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections* issued by President's Council on Integrity and Efficiency.

Appendix B
Management Comments to the Draft Report



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

Homeland
Security

April 20, 2009

MEMORANDUM FOR: Carlton I. Mann
Assistant Inspector General for Inspections

FROM: Jerry Levine
Director, GAO/OIG Audit Liaison Office

SUBJECT: Response to Draft Report: *Efforts to Identify Critical Infrastructure Assets and Systems*

We would like to thank you for allowing us the opportunity to provide a consolidated response on your draft report titled" Efforts to Identify Critical Infrastructure Assets and Systems". The comments and responses reflect the views of the National Programs and Protection Directorate (NPPD), Federal Emergency Management Agency (FEMA) and Immigration and Customs Enforcement (ICE).

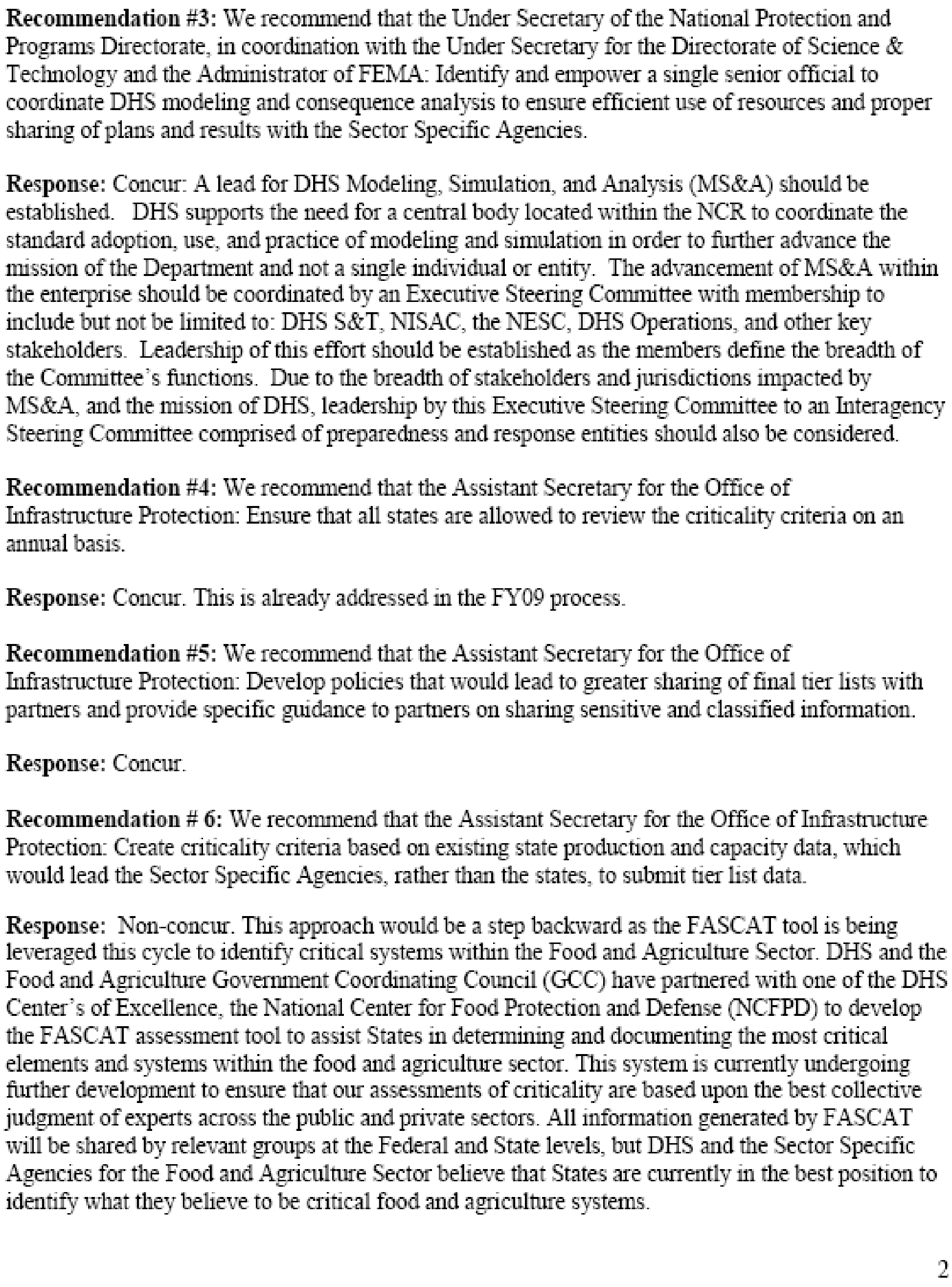
The following outlines the Department's response to the ten recommendations in the draft report.

Recommendation #1: We recommend that the Under Secretary for National Protection and Programs and the Under Secretary for Management: Complete the acquisition process for the Infrastructure Information Collection System.

Response: Concur. The Infrastructure Information Collection Division (IICD) will continue to implement the Infrastructure Information Collection System (IICS) as an improved approach to collecting and maintaining authoritative and reliable information on the nation's infrastructure, and looks forward to working with offices in the Under Secretary for Management, as identified in Recommendation #1 of the report.

Recommendation #2: We recommend that the Under Secretary of the National Protection and Programs Directorate, in coordination with the Under Secretary for the Directorate of Science & Technology and the Administrator of FEMA: Pursue and document additional budgetary resources to support necessary infrastructure modeling and consequence analysis as outlined in sectors' annual reports.

Response: Concur. Current projected funding levels will generally only support HITRAC requests for information and maintain most existing capability. Congressional requirements and changes in the NIPP provide the basis for the scope of capability that NISAC should provide to National/Federal, Regional, SSAs, and other NIPP partners. Providing this capability across the NIPP and the Integrated Planning System will require a dedicated effort to document total NISAC requirements.



Recommendation #3: We recommend that the Under Secretary of the National Protection and Programs Directorate, in coordination with the Under Secretary for the Directorate of Science & Technology and the Administrator of FEMA: Identify and empower a single senior official to coordinate DHS modeling and consequence analysis to ensure efficient use of resources and proper sharing of plans and results with the Sector Specific Agencies.

Response: Concur: A lead for DHS Modeling, Simulation, and Analysis (MS&A) should be established. DHS supports the need for a central body located within the NCR to coordinate the standard adoption, use, and practice of modeling and simulation in order to further advance the mission of the Department and not a single individual or entity. The advancement of MS&A within the enterprise should be coordinated by an Executive Steering Committee with membership to include but not be limited to: DHS S&T, NISAC, the NESC, DHS Operations, and other key stakeholders. Leadership of this effort should be established as the members define the breadth of the Committee's functions. Due to the breadth of stakeholders and jurisdictions impacted by MS&A, and the mission of DHS, leadership by this Executive Steering Committee to an Interagency Steering Committee comprised of preparedness and response entities should also be considered.

Recommendation #4: We recommend that the Assistant Secretary for the Office of Infrastructure Protection: Ensure that all states are allowed to review the criticality criteria on an annual basis.

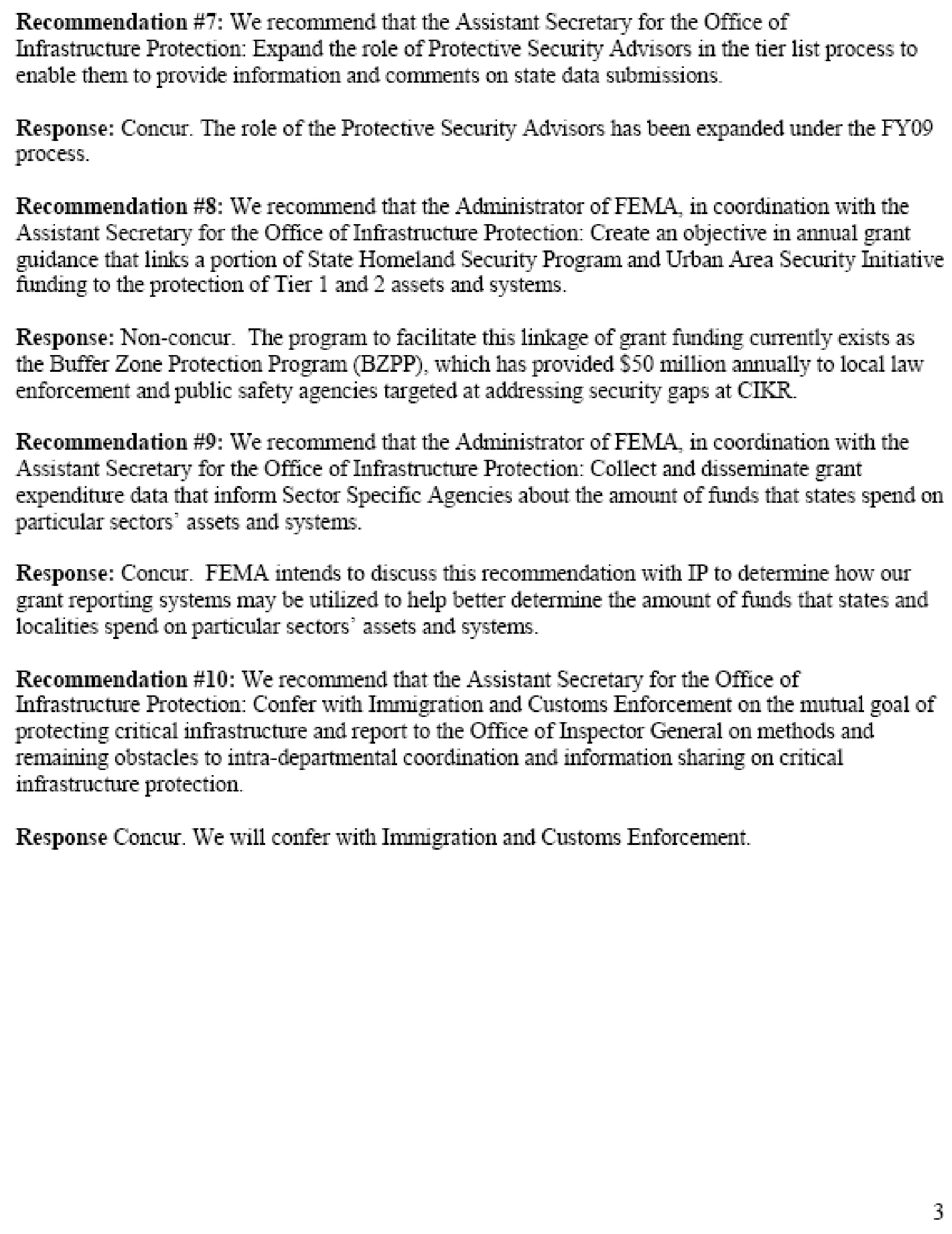
Response: Concur. This is already addressed in the FY09 process.

Recommendation #5: We recommend that the Assistant Secretary for the Office of Infrastructure Protection: Develop policies that would lead to greater sharing of final tier lists with partners and provide specific guidance to partners on sharing sensitive and classified information.

Response: Concur.

Recommendation # 6: We recommend that the Assistant Secretary for the Office of Infrastructure Protection: Create criticality criteria based on existing state production and capacity data, which would lead the Sector Specific Agencies, rather than the states, to submit tier list data.

Response: Non-concur. This approach would be a step backward as the FASCAT tool is being leveraged this cycle to identify critical systems within the Food and Agriculture Sector. DHS and the Food and Agriculture Government Coordinating Council (GCC) have partnered with one of the DHS Center's of Excellence, the National Center for Food Protection and Defense (NCFPD) to develop the FASCAT assessment tool to assist States in determining and documenting the most critical elements and systems within the food and agriculture sector. This system is currently undergoing further development to ensure that our assessments of criticality are based upon the best collective judgment of experts across the public and private sectors. All information generated by FASCAT will be shared by relevant groups at the Federal and State levels, but DHS and the Sector Specific Agencies for the Food and Agriculture Sector believe that States are currently in the best position to identify what they believe to be critical food and agriculture systems.



Recommendation #7: We recommend that the Assistant Secretary for the Office of Infrastructure Protection: Expand the role of Protective Security Advisors in the tier list process to enable them to provide information and comments on state data submissions.

Response: Concur. The role of the Protective Security Advisors has been expanded under the FY09 process.

Recommendation #8: We recommend that the Administrator of FEMA, in coordination with the Assistant Secretary for the Office of Infrastructure Protection: Create an objective in annual grant guidance that links a portion of State Homeland Security Program and Urban Area Security Initiative funding to the protection of Tier 1 and 2 assets and systems.

Response: Non-concur. The program to facilitate this linkage of grant funding currently exists as the Buffer Zone Protection Program (BZPP), which has provided $50 million annually to local law enforcement and public safety agencies targeted at addressing security gaps at CIKR.

Recommendation #9: We recommend that the Administrator of FEMA, in coordination with the Assistant Secretary for the Office of Infrastructure Protection: Collect and disseminate grant expenditure data that inform Sector Specific Agencies about the amount of funds that states spend on particular sectors' assets and systems.

Response: Concur. FEMA intends to discuss this recommendation with IP to determine how our grant reporting systems may be utilized to help better determine the amount of funds that states and localities spend on particular sectors' assets and systems.

Recommendation #10: We recommend that the Assistant Secretary for the Office of Infrastructure Protection: Confer with Immigration and Customs Enforcement on the mutual goal of protecting critical infrastructure and report to the Office of Inspector General on methods and remaining obstacles to intra-departmental coordination and information sharing on critical infrastructure protection.

Response Concur. We will confer with Immigration and Customs Enforcement.

3

Question 1: How long have you been a PSA?

Less than 90 days	1
3 to 6 months	0
More than 6 but less than 12 months	1
1 to 2 years	10
More than 2 years	51

Question 2: Regarding the annual List process, how do you judge the level of your involvement in vetting the information submitted by your state(s) to the Office of Infrastructure Protection?

I do not need to be more involved in helping states create asset lists	28
IP should ensure that I am more involved in helping states create asset lists	33

Question 3: Which statement below best expresses your view on the preferred level of private sector involvement in the vetting of list submissions and the review of the sectors' criticality criteria?

The private sector does not need to be more involved in the vetting of assets and the review of criteria	8
Some additional private sector involvement in these areas would be useful	32
A much greater level of private sector involvement is necessary in these areas	21

Question 4: Do states currently have sufficient opportunity to suggest revisions to the criticality criteria that IP provides to help guide list submissions?

Yes	21
No	30
I don't have an opinion	11

Question 5: Based on the choices below, what statement best reflects your view of the completeness of the data that states submit for purposes of populating the CIKR lists?

States are able to submit very complete data	13
If there are problems with incomplete list submissions, these concerns are minor and are not a long-term issue	17
IP needs to take significant steps to ensure that states are submitting more complete list submissions	25
I don't have an opinion on this matter	6

Question 6: On a scale of 1 (poor) to 5 (excellent), how do you rate the value and completeness of the current list criticality guidance provided by IP to states?

1	5
2	15
3	15
4	20
5	3

Question 7: On a scale of 1 (poor) to 5 (excellent), how well does the current process inform and improve overall risk management (grant funding, site visits, security improvements, etc.)

1	4
2	14
3	22
4	14
5	0

Question 8: On a scale of 1 (poor) to 5 (excellent), how do you rate the current efforts to ensure that "systems-based sectors" (e.g., food/agriculture, energy, banking/finance) are represented in the lists, in addition to sectors based more on fixed assets (e.g. nuclear, commercial facilities, dams)?

1	7
2	19
3	21
4	8
5	4

Question 9: Section 1001 of the 9/11 Commission Act allows, but does not require, DHS to establish a National Infrastructure Protection Consortium, which may advise

DHS on "the best way to identify, generate, organize, and maintain any database or list of systems and assets" created by DHS. Do you believe such a consortium would be beneficial, or do you believe current relationships, committees, and processes are sufficient?

The Consortium mentioned in the Act should be established because it could augment the work of identifying CIKR assets and systems	31
The Consortium is not needed because existing relationships and processes are sufficient in identifying CIKR assets and systems	30

Appendix D
Major Contributors to this Report

Douglas Ellice, Chief Inspector, Office of Inspections

Darin Wipperman, Senior Inspector, Office of Inspections

Kristine Odiña, Inspector, Office of Inspections

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Deputy Chiefs of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary, National Protection and Programs Directorate
National Protection and Programs Directorate Liaison
Office of Infrastructure Protection Liaison
Chief Security Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:

  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.