DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Progress in Developing the National Asset Database

Office of Inspections and Special Reviews

OIG-06-40

June 2006

Office of Inspector General

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

June 20, 2006

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 responsibility to promote economy, effectiveness, and efficiency within the department.

This report assesses the actions DHS has taken to identify and organize the nation's critical infrastructure and key resources in the National Asset Database. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

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

Richard L. Skinner
Inspector General

Contents

Executive Summary 1

Background 2

Results of Review 5

Identification and Collection of Critical Infrastructure and Key Resource Information 5

Concerns About State-Identified Assets 9

Prioritizing the National Asset Database 16

Enhancing Prioritization Capability 18

Recommendations 21

Management Comments and OIG Analysis 21

Appendices

Appendix A: Purpose, Scope, and Methodology 26
Appendix B: Preparedness Response to OIG 28
Appendix C: Roles and Responsibilities within NIPP Risk Management Framework 35
Appendix D: Critical Infrastructure and Key Resource Sectors 41
Appendix E: Guidelines for Identifying National Level Critical Infrastructure and Key Resources 42
Appendix F: Critical Infrastructure/Key Resource Totals By State 46
Appendix G: Major Contributors to This Report 48
Appendix H: Report Distribution 49

Abbreviations

BZPP	Buffer Zone Protection Program
CI/KR	Critical Infrastructure/Key Resources
CIP-DSS	Critical Infrastructure Protection-Decision Support System
COP	Common Operational Picture
GCOA	Gross Consequences of Attack
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSA	Homeland Security Act of 2002
HSOC	Homeland Security Operations Center
HSPD	Homeland Security Presidential Directive
IA	Office of Intelligence and Analysis
IAIP	Information Analysis and Infrastructure Protection Directorate
IP	Office of Infrastructure Protection
LNG	Liquefied Natural Gas
NADB	National Asset Database
NICC	National Infrastructure Coordination Center
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NRC	National Response Center
NSHS	National Strategy for Homeland Security
NSPP	National Strategy for the Physical Protection of Critical Infrastructure and Key Assets
ODP	Office for Domestic Preparedness
OIG	Office of Inspector General
PCCIP	President's Commission on Critical Infrastructure Protection
PCII	Protected Critical Infrastructure Information Program
PDD	Presidential Decision Directive
PMTL	Protective Measures Target List
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RMD	Risk Management Division
SSA	Sector Specific Agency
UASI	Urban Area Security Initiative
USCG	United States Coast Guard
USACE	United States Army Corps of Engineers

Executive Summary

On December 17, 2003, President Bush released Homeland Security Presidential Directive No. 7, *Critical Infrastructure Identification, Prioritization, and Protection* - a national policy for federal departments and agencies to identify and prioritize the United States' critical infrastructure and key resources (CI/KR) and to protect them from terrorist attacks. The Department of Homeland Security (DHS) is responsible for establishing the risk management framework necessary to coordinate these efforts. This framework requires the support of a comprehensive, national asset inventory. DHS calls this inventory the National Asset Database (NADB).

DHS' Office of Infrastructure Protection (IP) is still identifying and collecting CI/KR data, simultaneously populating the first-generation NADB, and building the next-generation NADB. As of January 2006, the NADB contained 77,069 assets, which are not distinguished by criticality. Only after IP completes risk assessments of the assets will it have actual lists of CI/KR. Nonetheless, the varying presence of non-critical assets - and they are difficult to quantify – confirms that the NADB is not an accurate representation of the nation's CI/KR. In addition, the NADB is not yet comprehensive enough to support the management and resource allocation decision-making envisioned by the National Infrastructure Protection Plan (NIPP).

IP has a substantial amount of work ahead to determine the ultimate disposition of the NADB's contents and each asset's importance to the country. It is working on enhancing its ability to analyze and prioritize CI/KR data but those efforts continue to be affected by slow development of both the NADB and risk assessment tools. We cannot predict when IP will have both the data and the analytical tools to provide a comprehensive risk assessment of the country's critical infrastructure and key resources.

We are recommending four specific actions to the Under Secretary for Preparedness to improve the development and quality of the national asset database.

Background

In 1998, President Clinton issued Presidential Decision Directive No. 63 (PDD-63), *Critical Infrastructure Protection*, which set forth principles for protecting the nation by minimizing the threat of smaller-scale terrorist attacks against information technology and geographically-distributed supply chains that could cascade and disrupt entire sectors of the economy.[1] Absent a centralized authority for homeland security, federal agencies were designated as Lead Agencies in their sector of expertise. The Lead Agencies were tasked to develop sector-specific Information Sharing and Analysis Centers to coordinate efforts with the private sector. PDD-63 required the creation of a National Infrastructure Assurance Plan.

The present administration was reviewing this strategy when the terrorist attacks of September 11, 2001, accelerated its implementation. It began to adapt and develop the principles of PDD-63. Executive Orders 13228 and 13231 expanded the federal role as a coordinating partner for state and local agencies as well as the private sector, raised the priority of physical assets as distinguished from cyber assets, and organized infrastructure coordination through the creation of the National Infrastructure Advisory Council, the Homeland Security Council, and the Office of Homeland Security.[2]

In July 2002, the White House Office of Homeland Security released the National Strategy for Homeland Security (NSHS). Protecting the nation's critical infrastructure and key assets was one of its six critical mission areas.[3] Critical infrastructure was previously defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters…."[4] The NSHS adds to this concept a concern for key assets, "individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence. Key assets include symbols or historical attractions,

[1] *Presidential Decision Directive 63: Critical Infrastructure Protection*, May 22, 1998. Executive Order 13010: Critical Infrastructure Protection, established the President's Commission on Critical Infrastructure Protection (PCCIP). Federal Register Vol. 61, No. 138, July 17, 1996, pp. 37347-37350. PCCIP fostered the development of PDD-63.
[2] Executive Order 13228: Establishing the Office of Homeland Security and the Homeland Security Council, Vol. 66, No. 196, Oct. 10, 2001. pp. 51812-51817. Executive Order 13231: Critical Infrastructure Protection in the Information Age. Federal Register. Vol. 66, No. 202. Oct. 18, 2001. pp. 53063-53071.
[3] National Strategy for Homeland Security, pp. viii, 29-36.
[4] *USA PATRIOT Act*, P.L. 107-56 Sec. 1016(e).

such as prominent national, state, or local monuments and icons."[5] This differs slightly from the term "key resources," defined in the *Homeland Security Act of 2002* (HSA) as "publicly or privately controlled resources essential to the minimal operations of the economy and government."[6] The NSHS continued the concept of lead agencies—now called Sector-Specific Agencies (SSAs)—but designated the yet-to-be-created DHS to coordinate the strategy as well as be the lead agency for some sectors. It defined eight major initiatives in protecting critical infrastructure and key assets, including "[b]uild[ing] and maintain[ing] a complete assessment of America's critical infrastructure and key assets."[7]

The HSA created DHS. Within DHS's Information Analysis and Infrastructure Protection Directorate (IAIP), the Office of Infrastructure Protection (IP) assumed responsibility for assessing the nation's critical infrastructure and key resources.[8] IAIP was responsible for accessing and integrating information from the federal government, state, and local government agencies, and private sector entities in order to "identify and assess the nature and scope of terrorist threats to the homeland."[9] Additionally, it was responsible for developing and coordinating a comprehensive national plan to secure critical infrastructure and key resources. This includes assessments of risk, integrating "relevant information, analyses, and vulnerability assessments… in order to identify priorities for protective and support measures…."[10]

Within a month of its establishment, in February 2003, DHS took steps toward developing a national plan by issuing the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. This document identified the leadership role of the federal government in "[t]aking stock of our most critical facilities, systems, and functions…" and required DHS to: (1) "[d]evelop a uniform methodology" for identifying critical assets; (2) "[b]uild a comprehensive database to catalog these critical facilities, systems, and functions"; (3) maintain an "up-to-date assessment of vulnerabilities and preparedness across critical sectors"; and, (4) establish a

[5] NSHS p. 30.
[6] *Homeland Security Act*, P.L. 107-296, Sect. 2(9).
[7] NSHS, p. 33.
[8] HSA, Sect. 201(d)(2) assigned responsibility for assessing CI/KR to IAIP. When DHS reorganized in 2005 and IAIP's two primary components, the Office of Information Analysis (IA) and the Office of Infrastructure Protection, were split. IA was renamed the Office of Intelligence and Analysis, and now reports directly to the Secretary. IP retained its name and was moved to the Preparedness Directorate. The Assistant Secretary for Infrastructure Protection leads IP.
[9] HSA, Sect. 201(d)(1)(A).
[10] PL 107-296, Sect. 201(d)(3).

multi-year approach for critical infrastructure and key asset protection to "instill predictability and structure in the planning process."[11] Developing a geospatial mapping of critical infrastructure and key resources was a separate but related part of the strategy.[12]

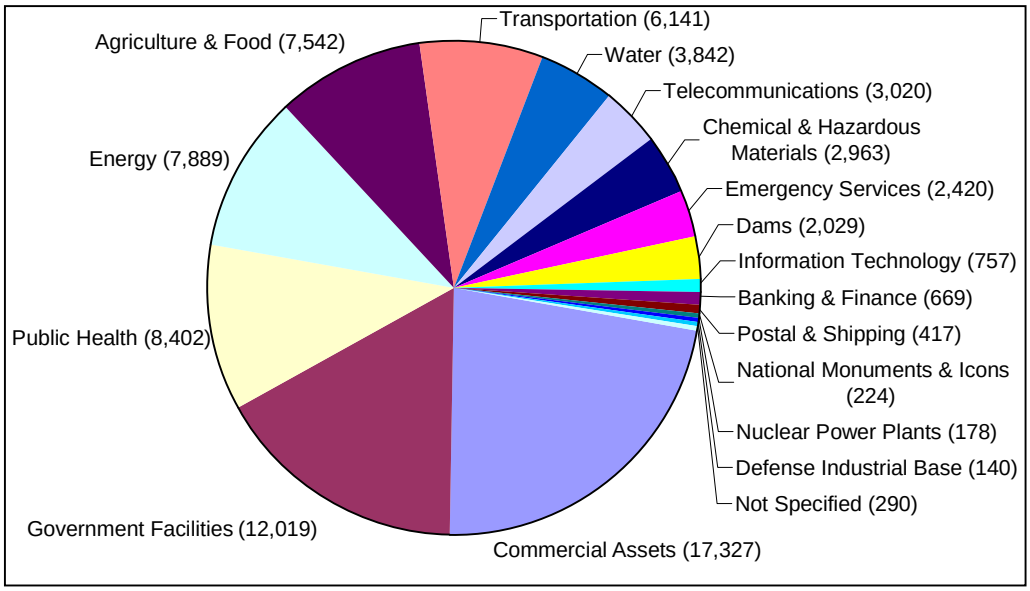
In December 2003, this over-arching strategy became policy in Homeland Security Presidential Directive No. 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection.* HSPD-7 sets forth the Secretary of Homeland Security's role in setting "uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities," based on critical infrastructure for which DHS, including IP, will "identify, prioritize, and coordinate the protection."[13] The HSPD-7 required DHS to detail a national plan for CI/KR protection within one year; DHS did not meet this deadline.[14]

The development of the National Infrastructure Protection Plan (NIPP) has taken longer than expected, with an interim NIPP released in February 2005 and a draft version of the final NIPP made available for public comment in November 2005 (as of this report, DHS had not released a final NIPP). The draft NIPP draws on the key elements of HSPD-7 in its risk management framework, which involves the following stages: 1) identification of critical infrastructure; 2) identification and assessment of vulnerabilities; 3) normalization, analysis, and prioritization; 4) implementation of protective programs; and, 5) measuring effectiveness. Federal, state and local, and private sector entities all have a role in implementing this framework (see Appendix C). The NIPP envisions a comprehensive, national inventory of assets to support its framework. DHS calls this inventory the NADB.

The NADB is intended to be a "comprehensive catalog that includes an inventory and descriptive information regarding the assets and systems that comprise the nation's CI/KR."[15] DHS is now focused on populating the first-generation NADB, the national asset inventory that will support the development of an informed national risk profile. The current NADB is diverse and includes entries under every category of CI/KR (see Chart 1).

[11] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003. p.ix and p.23.
[12] NSPP CI/KA. pp. 24.
[13] *Homeland Security Presidential Directive/ HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection*, Dec. 17, 2003.
[14] DHS also missed additional deadlines for reports on risk assessment and readiness enacted in the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458.
[15] Draft NIPP, November 2005, Section 3.2.1, p. 29. This document is pre-decisional.

Chart 1: NADB Totals by Sector



For example, the inventory includes 4,055 malls, shopping centers, and retail outlets; 224 racetracks; 539 theme or amusement parks and 163 water parks; 514 religious meeting places; 4,164 educational facilities; 1,305 casinos; 234 retail stores; 127 gas stations; 130 libraries; 335 petroleum pipelines; 217 railroad bridges; 140 defense industrial base assets; 224 national monuments and icons; and 8 wind power plants. In addition to hosting the national asset inventory, the current NADB is integrating information available in various DHS and other federal databases using a single portal with a common interface.

Results of Review

Identification and Collection of Critical Infrastructure and Key Resource Information

The NADB began as a small list of assets. In summer 2003, IP's Risk Management Division (RMD) (known then as the Protective Security Division), which oversees the NADB program, applied gross consequences and significant economic impact criteria to identify 160 nationally critical

assets as part of Operation Liberty Shield.[16] Later that year, under pressure from Congress to produce a prioritized list, IP identified more assets and expanded the list to 1,849.[17] IP identified assets in specific sectors—chemical, hazardous material, nuclear, business and finance, electric, oil and natural gas, transportation, commercial, and government facilities—that it determined required additional protection or mitigation against terrorist attacks. It was called the Protected Measures Target List (PMTL).[18] Subsequently, the Office of Domestic Preparedness (ODP) asked state and local governments to provide critical infrastructure data as part of a state self-assessment program.[19] By February 2004, that data was combined with the PMTL to become a national asset list of 28,368 assets. The list did not adequately represent the nation's 13 critical infrastructure sectors and 4 key resources (see Appendix D).

In July 2004, IP initiated a data call to states and territories for critical infrastructure and key resource information. Between July 2004 and July 2005, states identified and submitted data for 48,701 assets. States tried to follow DHS' criteria for identifying national critical infrastructure and key resources, but their submissions were inconsistent and often delayed. IP included every submitted asset in the NADB in order to make it as comprehensive as possible. IP went to considerable effort to process, format, and verify this information, even eliminating 3,846 duplicate submissions between the two data calls. The NADB is considered the official database and these initiatives combined generated a total of 77,069 assets (see chart 2).[20] However, IP has access to, and is pursuing, asset information in other federal and commercial repositories that it can link to the NADB, which could increase the number of assets in the NADB by hundreds of thousands.

[16] Operation Liberty Shield was a comprehensive national plan to protect critical infrastructure while Operation Iraqi Freedom was executed overseas. IP selected the assets based on a risk assessment. The risk assessment considered sites that if attacked could produce consequences of national scale, primarily significant loss of life or catastrophic damage to the economy. Then-DHS Secretary Ridge asked governors to protect these assets.

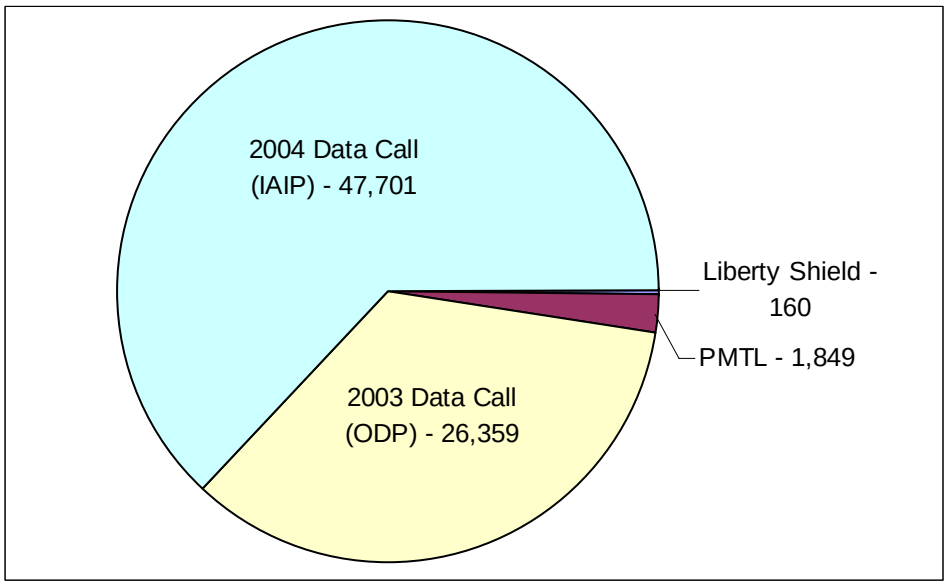
[17] Officials both in and out of DHS frequently referred to the "list of 1,700." Based on feedback from States, IP subsequently expanded the list to 1,849.

[18] The 1,849 assets became the focus of, and a starting point for, IP's Buffer Zone Protection Program.

[19] Last year RMD began adding the source of each entry in the NADB. We learned late in our review that many sources of data were culled as part of the state assessments and to help prepare the national inventory list. Examples included several "DHS Lists," the "Chemical Sites List," "GSA Buildings," "ME Critical Assets, Systems, and Infrastructure," and "Largest Water Utilities."

[20] The NADB is housed at a national laboratory.

Chart 2: NADB Totals by Stages of Development



Processing State Submissions Has Been Difficult

States took more than a year to compile information for 17 fields of identification and location data on each asset to complete their submissions. IP then needed time to resolve numerous formatting issues with the data. IP set a deadline of October 1, 2004, to submit responses but underestimated how much time states would require and the level of difficulty involved. Only 2 of 56 states and territories met that deadline. The timeliness of the submissions was dictated by each state's approach, how much it already knew about critical infrastructure (some states did not have a database of critical infrastructure), how it interpreted IP's criteria, and whether there were legal obstacles to forwarding CI/KR information on private sector assets. Some states did not share information with DHS immediately because state legislation prevented disclosure. It was not unusual for states to send multiple submissions to IP, and for the content of their responses to vary.

IP hired a contractor to format and verify data for thousands of assets. It encountered numerous obstacles. For example, states (1) submitted data in different formats; (2) omitted facility names; (3) submitted duplicate assets (for example, an asset located on a state line is submitted by both states); and, (4) used inconsistent zip codes. Puerto Rico's data had to be translated because it was prepared in Spanish. A significant challenge was finding

missing information about assets. IP deemed data fields such as state, address, sector, owner, owner type, phone, local law enforcement POC, and latitude and longitude coordinates as critical. Officials estimated that on average each CI/KR record they researched was missing information for about seven fields. By December 2004, the contractor had completed research on 13 states. In the summer of 2005, IP hired another contractor to perform the critical task of verifying the location of each asset, which it did, by December 2005. [21]

Criteria for Identifying CI/KR is Improving

The guidance DHS gave to states for the 2003 ODP-led data call was minimal. It required that states "….[T]ake immediate action to identify and increase the security of critical infrastructure and key assets within your state. In selecting such infrastructure you should consider any system or asset that if attacked would result in catastrophic loss of life and/or catastrophic economic loss."[22] It also identified specific types of facilities that states should consider while identifying CI/KR.[23]

IP expanded and improved upon ODP's criteria for its July 2004 data call. It sent to states the "*Guidelines for Identifying National Level Critical Infrastructure and Key Resources"* for the 13 critical infrastructure sectors and 4 key resources. The guidelines identified more categories of CI/KR and accompanying parameters or subcategories (see Appendix E). For example, they included subcategories such as "major banking and financial centers," "refineries with refining capacity in excess of 225,000 barrels per day," "primary medical care facilities with unique services," "IT systems with access or control points distributed on both coasts and throughout the country," and "commercial centers with potential economic loss impact of $10 billion or capacity of more than 35,000 individuals." DHS kept the criteria general to encourage states to submit any asset they thought to be important.

In August 2005, the Assistant Secretary for Infrastructure Protection approved the NADB taxonomy. IP solicited input from all CI/KR sectors, and federal departments and agencies made substantial contributions to its development.

[21] Several contractors have been actively involved in the development of the NADB, a gross consequences of attack prioritization methodology, and software for accessing the NADB as well as housing the NADB and coordinating expert panels to assess the NADB.
[22] Criteria for the selection of critical infrastructure, ODP, 2003.
[23] For example, facilities included public water systems, primary data storage and processing, chemical, major power generation, nuclear power plants, electric substations, rail and highway bridges, natural gas and liquid natural gas storage, and major mass transit subway systems.

IP officials view the new taxonomy as the driving architecture behind the next-generation NADB because it standardizes the terminology that DHS, sector-specific agencies, states and territories, and private industry will use to categorize and subcategorize national infrastructure. It uses multiple levels of detail, defines attributes of interest for each level, and notes other possible categorizations for an asset. For example, the agriculture & food sector is broken down into numerous subcategories including supply, processing, packaging, and production, product storage, product transportation, distribution, and supporting facilities. The taxonomy does not perform any risk analysis; it does not assign values to the specific attribute data or determine each asset's national significance. IP has not yet applied the taxonomy to categorize assets in the NADB, or shared it with the states.

Concerns About State-Identified Assets

Both data calls generated an abundance of unusual, or out-of-place, assets now in the NADB whose criticality is not readily apparent. There are also inconsistencies when comparing state-by-state asset totals. Furthermore, the NADB indicates 32,631 of its assets are not nationally significant, outnumbering the nationally significant assets 3 to 1. While it is not IP's intent at this stage to specifically assign criticality or identify the most critical assets—it is still focusing on collecting data to develop the national asset inventory—their presence complicates efforts to develop a useful, first-generation database. Ambiguity about what constitutes a CI/KR could lead to inefficient use of limited homeland security resources.[24]

IP officials share our concern about the quality of the NADB and whether DHS is directing resources to the most significant CI/KR. IP officials believe it is essential that the NADB retain any asset that could be a terrorist target in order for it to properly support the NIPP. IP asked states to identify their nationally significant assets but at the same time did not discourage them from submitting any asset. This information will help with the national risk profile as well as provide the capability to map threat data against critical infrastructure in a geospatial environment. Testifying before Congress, the former Under Secretary for IAIP remarked, "We take the intelligence that we get day-to-day and we share it from IA to IP, so we track, or what we call map, the intelligence against the 1,700 [assets] …and then broadly speaking,

[24] Congressional Research Service: Critical Infrastructure and Key Assets: Definition and Identification, October 2004.

across this larger database of 28,000 sites."[25] IP will gather additional information on those assets it determines to be nationally significant. Per the NIPP, examples of this information include vital system components, dependencies and interdependencies, existing protective measures, worst reasonable case consequences, and quantitative consequence analysis.

Out-of-place assets make resource allocation decisions more challenging; every possible target is not going to rise to the level of national significance. IP plans on filtering those assets from the NADB with the individual analyses for each program or sector. However, having more assets may obscure desired data, making such prioritizations more difficult. Additionally, assets that will never be used in an analysis will have to be filtered out repeatedly. Both of the department's recent data calls generated many assets now in the NADB whose national significance is questionable and IP might waste time and resources trying to prioritize them.

State Responses to Criticality Question Were Inconsistent

DHS also requested states to designate those assets that "met national level criteria." In deciding which assets to submit, states had considerable latitude in interpreting what DHS meant by a nationally critical asset. States assessed potential catastrophic loss, economic impact, public confidence or national symbolism, and replaceability to identify the assets. The NADB currently shows that 11,018 assets (14 percent) rise to the level of nationally significant, while 32,631 assets (42 percent) do not. The question of national significance is undetermined for another 33,419 assets (43 percent).[26] IP officials acknowledge that many assets will never be analyzed in depth or used to support any program activity.

Some states submitted assets that they knew were critical to the state but were not sure about their national importance, and some did not. States that adopt an all-hazards approach to infrastructure protection consider schools as critical to the general public's safety during a natural disaster because they function as emergency shelters. However, states did not consistently submit schools because they did not know whether they warranted inclusion in the NADB. The lack of guidance on whether questionable categories of

[25] General Frank Libutti, testifying before the House Appropriations Subcommittee on Homeland Security on DHS FY2005 Appropriations, April 1, 2004.
[26] To the best of our knowledge, the question of national significance was not incorporated into ODP's data collection efforts in 2003. While these figures suggest otherwise, DHS is in the process of filling these fields for each asset.

assets (such as schools) should be included led to significant variation in submissions, and decreases the value of comparisons across states.

In addition, the NADB contains general categories because DHS did not provide guidance for naming assets by level of specificity. For example, states were not sure whether to simply identify a subway system by name, or name each important facility or station within that system. Instead of a specific school, some locations listed schools in general. Other generalities include restaurants and churches. There are inherent challenges in capturing systems and asset data simultaneously. At present, the NADB is not structured in a way that enables it to capture information about systems. Even if the categories above are reasonable, the NADB requires a consistent approach listing the specific assets to be a useful tool. The NADB taxonomy is the first step in delineating and creating a consistent approach to listing assets, systems and networks across the SSAs and down to the local level.

Portion of NADB Populated by First Data Call Lacks Credibility

The 2003 ODP-led data call generated 28,368 assets. The presence of large numbers of out-of-place assets taints the credibility of the data (see examples in Table 1). The states' unfamiliarity with identifying CI/KR, and DHS' lack of direction contributed to the poor quality of the data.

Table 1: Examples of Out-of-Place Assets (ODP 2003 Data Call)

Old MacDonald's petting zoo	Mall at Sears
Bean Fest	Nix's Check Cashing
Amer. Society of Young Musicians	Trees of Mystery
Car Dealerships	Kennel Club and Poker Room
Historical Bok Sanctuary	4 Cs Fuel and Lube
DPW Landfill	Kangaroo Conservation Center
Assyrian American Association	[state] Right to Life Committee
Association for the Jewish Blind	[university] Insect Zoo
Bourbon Festival	Theological Seminary
Jay's Sporting Goods	Nestle Purina Pet food Plant
Auto Shop	Veterinary Clinic
Groundhog Zoo	Sweetwater Flea Market
High Stakes Bingo	Petting Zoo
[state] Community College	[a] Restaurant
Frontier Fun Park	[a] Travel Stop
Mule Day Parade	Beach at End of [a] Street
Amish Country Popcorn	[a] Pepper and Herb Company

State officials had little knowledge about the first data call, and did not know that it resulted in lists of assets that were included in DHS' national asset inventory. In fact, officials were repeatedly surprised to learn about the existence of another batch of assets from their state in the NADB. One state official remarked that the list should be deleted. DHS did not appear to have communicated its intentions to add those assets to the NADB. State officials said they would seek clarification from IP as to their respective total number of assets in the NADB. One state official commented that he was told by DHS that the data was in the NADB because DHS needed to begin preparing a prioritized list of national critical infrastructure and it was going to use this information if states did not adequately respond to the 2004 data call.

Since we began monitoring the development of the NADB, IP officials have asserted that the older data was of low quality and that they had little faith in it. They claimed not to know what criteria ODP used.[27] We received scant information detailing those criteria. However, based on the origins of the data, the subjective criteria used, the process used to collect the data, the states' lack of knowledge, and in some cases denial of those lists, IP should examine the data to identify those assets that other sources find insignificant. It should receive cooperation from state officials, who said definitively that they want to have more input on their assets in the NADB.

July 2004 Data Call Included Some Curious Assets

The July 2004 data call was significantly more organized and achieved better results than the previous data call. IP provided sector-specific parameters to help states identify the assets it wanted and encouraged states to submit any asset they thought was important (see Appendix E). IP expected states would value sectors differently, and states did arrive at different conclusions about which assets, and how many, were nationally significant. Their responses also varied because of a lack of understanding of critical systems on a national level. States that pursued every asset thought to be a potential target may have submitted assets that are not in fact nationally significant.

Although it generated more relevant assets, the 2004 data call included noticeable out-of-place assets, especially among those assets designated as non-nationally significant (see Table 2). We examined in more detail the NADB's list of assets for Florida, Illinois, Indiana, and Maryland (we visited

[27] ODP officials provided evidence that they collaborated with infrastructure protection officials during the state assessments and both organizations prepared the criteria.

all but Indiana) and identified several questionable soft and hard target assets.[28]

Table 2: Examples of Out-of-Place Assets From Four States (July 2004 Data Call)

Psychiatry Behavioral Center	Order of Elks National Memorial
Ice Cream Parlor	Bakery & Cookie Shop
Inn	Donut Shop
Sears Auto Center	Wine and Coffee Co.
Sports Club	Casket Company
Bass Pro Shop	Muzzle Shoot Enterprise
Several Wal-Marts	Property Owners Associations
Apple and Pork Festival	Rolls Royce Plant
Pepsi Bottlers	Yacht Repair Business
Anti-Cruelty Society	Tackle Shop
Elevator Company	Center for Veterinary Medicine
American Legion	UPS Store
Heritage Groups	Parcel Shop
YMCA Center	Brewery
Mail Boxes Etc	Night clubs

While discussing the goals of July 2004 data call, state officials consistently said that they preferred to have a manageable list of critical infrastructure within their state over a larger, less accurate, and less relevant list. They acknowledged concern that they showed too much restraint and underreported critical infrastructure. The totals states reported support the belief that there is more CI/KR information that states could have reported which would be relevant to DHS. Florida officials stated that they did not submit schools for the NADB, even though they serve a vital role as shelters during natural disasters.

Data Calls Resulted in Inconsistent State-by-State Totals

Together, the ODP-led 2003 data call and the July 2004 data call resulted in peculiar totals when comparing sectors or states. There was significant variation in which CI/KR states considered important with (1) total reported assets varying widely by state (the standard deviation was higher than the average number of reported assets); and, (2) states reporting quirky totals in particular sectors. Compared to the more risk-based considerations of the Buffer Zone Protection Program (BZPP), it appears this was due to

[28] Soft targets include places for large assemblies and gatherings, e.g. stadiums and outdoor areas such as those used for Independence Day celebrations. Hard targets are usually defined as having security on site, standoff distance, fences, or cameras.

differences in reporting standards more than differences in risk.[29] This is true for both total assets (a complete listing is contained in Appendix F) and for assets reported in various sectors. For example:

- Indiana lists 8,591 assets in the NADB, more than any other state and fifty percent more than New York (5,687).

- California has 3,212 assets, fewer than 7 other states including Nebraska (3,457), Wisconsin (7,146), and Indiana (8,591).

- Vermont and New Hampshire have only 70 and 77 assets respectively. By comparison, Wisconsin and Indiana have a hundred times as many assets (7,146 and 8,591 respectively), almost all of which were submitted in the July 2004 data call.

- There is substantial inconsistency in reporting subway systems. California lists the entire Bay Area Regional Transit system as one item, while New York lists 739 stations, and Illinois lists more general categories, such as "CTA-Train" and "CTA-Terminal."

- Schools submitted include colleges, high schools, elementary schools, even kindergartens and Head Start programs. Reporting varies, as Virginia totals 2,126 schools while eight states or territories list none. The national total of 4,164 reported schools represent less than five percent of the approximately 96,000 public schools in America, and a cursory review does not suggest that they were chosen based on any consistent criteria.[30]

Comparing sectors also revealed inconsistency, in both national criticality and state reporting. For example:

- Some classes of assets where national criticality needs to be determined include 1,305 casinos, 25 golf courses, 24 swimming pools, 44 recreational centers and 163 water parks. Other asset types and quantities reported included 130 public libraries, 159 cruise ships, 34 Coca Cola bottlers/distributors, 244 correctional facilities, 718

[29] DHS initiated the Buffer Zone Protection Program to help address security concerns at the nation's most critical facilities. The program initially targeted the first 1,700 assets in the NADB. The BZPP is a local plan that aims to extend the zone of protection out from the facility fence and into the community in order to take the operational environment away from terrorists.

[30] Digest of Education Statistics Tables and Figures, 2004 (http://nces.ed.gov/programs/digest/d04/tables/dt04_005.asp).

mortuaries, 571 nursing homes, and 3,773 malls, of which only 399 met DHS' criteria of over 1 million square feet.

- Indiana and Wisconsin reported 77 times more agricultural assets than neighboring Illinois and Minnesota, even though Illinois and Wisconsin produce 50 percent more agricultural output with similar crops.[31]

- Nebraska listed 17 times as many emergency services as neighboring Iowa.

- Indiana lists 5,456 assets in the public health sector, or 65 percent of the sector total. The criticality of these assets, which included 417 nursing homes, is not clear.

- Illinois, home to some of the nation's tallest buildings in its city of Chicago, listed 28 tall buildings or just two-thirds as many as the 41 reported in Indiana.

- Washington lists 65 national monuments and icons, while Washington, D.C. lists only 37.

- New York lists only two percent of the nation's banking & finance sector assets, ranking between North Dakota and Missouri.

- New Mexico contained 73 percent of the information technology sector with 553 assets. The next highest state was Virginia with 68.

Inconsistent reporting, varying both between states and within states between asset categories, makes comprehensive analysis difficult. Additional data calls with clearer guidance should help states deliver comparable totals in all asset categories.

[31] According to the Economic Research Service (USDA) State Data Sheets- viewed at http://www.ers.usda.gov/StateFacts/IN.htm, http://www.ers.usda.gov/StateFacts/WI.htm http://www.ers.usda.gov/StateFacts/IL.htm, and http://www.ers.usda.gov/StateFacts/MN.htm.

Prioritizing the National Asset Database

As the Chairman of the House Appropriations, Subcommittee on Homeland Security noted, "Without a comprehensive and current inventory of our nation's critical infrastructure and key assets and a coherent picture of threats, the department's efforts to implement the appropriate protective measures, deploy the right technologies and make the right decisions about grant allocations are severely hampered."[32] IP currently does not intend to create a single prioritized list of infrastructure, but rather to prepare a comprehensive risk analysis of CI/KR as required by HSPD-7, highlighted in the NIPP, and requested by Congress. This analysis will be reflected in several, overlapping grant programs.[33] The NIPP's risk management framework includes an approach to integrate these prioritizations, stating "[DHS will] aggregate and order assessment results to present a comprehensive picture of national CI/KR risk in order to establish protection priorities and provide the basis for planning and the informed allocation of resources."[34]

Last year, the Government Accountability Office found that "DHS has begun developing, but has not yet completed, a framework to help agencies and the private sector develop a consistent approach for analyzing and comparing risks to transportation and other sectors. Until this framework is finalized and shared with stakeholders, it may not be possible to compare risks across different sectors, prioritize them, and allocate resources accordingly."[35] Presently, the NADB enables DHS to conduct consequence-based prioritization through "simple analytical normalization tools to convert risk assessment results into comparable units."[36]

IP initially prioritized the Protected Measures Target List, the upper echelon list of 1,849 assets identified based on perceived threats and consequences, but later determined that the ranked list was unreliable. The NADB is not prioritized and is not intended to be, but rather serves as a resource for the development of other prioritized lists. The NIPP states that, "Although the NADB is not, in and of itself, a listing of prioritized assets, it has the

[32] Chairman Harold Rogers' opening remarks during a hearing of the House Appropriations Subcommittee on Homeland Security on DHS FY2005 Appropriations, April 1, 2004.
[33] Attempts to consolidate these grant programs in order to present a more comprehensive picture of national infrastructure efforts under the Targeted Infrastructure Protection Program (TIPP) have not been approved by Congress.
[34] Draft National Infrastructure Protection Plan, November 2005, p.26.
[35] Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts, Highlights of GAO-05-851, found at http://www.gao.gov/new.items/d05851.pdf. The 'framework' is DHS' Risk Analysis and Management for Critical Asset Protection (RAMCAP) tool.
[36] Draft NIPP, p. 37.

capability to be queried in a variety of manners that can help inform…risk reduction activities."[37]

Several of DHS' protection programs utilize information from the NADB to help allocate resources. However, in light of the variation in reporting between various sectors and states as well as the lack of detailed information on sites, we are not confident that the NADB can yet support effective grant decision-making. We learned that DHS factored CI/KR data into funding decisions for several grant programs including the Urban Area Security Initiative (UASI), the Port Security Grant Program, and the Buffer Zone Protection Program (BZPP), but only the BZPP was directly supported by the NADB. In FY2005, the NADB was used in limited support of grant decisions because managers were not familiar enough with, or did not trust the accuracy of, the NADB's 77,069 assets. For UASI grants, DHS relied on other selected sector data where the source was deemed more reliable and detailed, e.g. known chemical plants. The Port Security Grant Program took into account data from the USCG rather than the NADB. The BZPP focused on CI/KR that comprised the Protected Measures Target List. In FY 2006, the NADB was used to a larger extent, although not exclusively.

DHS has not yet accomplished its goals for the first-generation NADB. IP is still building and populating the first-generation NADB to function as the official repository of national-level asset information. According to the NIPP, the first-generation NADB should support the following activities: (1) identifying and cataloging of specific attribute information necessary for risk-reduction analysis; (2) development of a comprehensive picture of the nation's critical infrastructure across all sectors; (3) use of a consequence-based prioritization process; (4) integration of a geospatial capability into the NADB; and (5) integration of data and results from research organizations, such as work performed by the National Infrastructure Simulation and Analysis Center (NISAC), through a single portal.[38] The first NADB has met some success in supporting the first element, but it is unclear when it will be able to support the remaining elements. DHS estimates it will not complete the next-generation NADB, which will fully incorporate information contained in other relevant databases, for at least two more years.[39]

[37] Draft NIPP, p. 81.
[38] Draft NIPP, p.82.
[39] Draft NIPP, p.87.

Enhancing Prioritization Capability

To effectively prioritize the NADB, DHS needs to be able to objectively compare each asset's criticality. Accordingly, IP intends to establish values with respect to human health and safety, economic value, iconic or symbolic value, and substitutability to model the value of dissimilar assets. Weighing these concerns, or normalizing assets, requires subjective determinations, for example, quantifying the symbolic value of the Statue of Liberty, and would require significant deliberation to develop tools to support a comprehensive national risk analysis.

IP has several ongoing tasks that should enhance its ability to prioritize assets across sectors. Specifically, IP is acquiring more and better data by purchasing or licensing data, directing SSAs to identify their most important assets, conducting gross consequence of attack analysis on the NADB, gathering expert panels to evaluate CI/KR data in the NADB, developing a standard risk assessment tool, and studying interdependencies across sectors. IP also seeks to collect as much data as possible in order to help develop a common operational picture (COP) via geospatial mapping of CI/KR. This includes integrating consequence, vulnerability, and threat information to provide a single risk analysis. By linking conditional risk with real time intelligence in the National Threat Incident Database, the NADB will support operational risk assessments. Analysts in DHS' Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) are responsible for fusing credible threat information received from the Office of Intelligence and Analysis (IA) with consequence assessments and vulnerability information provided by IP. HITRAC passes the results of its analysis back to IA and IP.[40]

These are meaningful steps toward producing a comprehensive national risk analysis, and they attest to the complexity of developing the NADB. IP has been planning or working on these measures for months and we hesitate to predict when DHS will have a functional and useful NADB. IP's progress in developing the NADB may affect key implementation milestones of the NIPP.

Acquiring Data. Significant amounts of data have already been incorporated into the NADB, and as we reported earlier, there may be too many lower priority assets. However, there is also concern that the NADB may have too few assets in essential areas and may present an incomplete picture. IP faces challenges in developing a comprehensive inventory due to both varying state

[40] Draft NIPP, p.58.

reports and reluctance of the private sector to share proprietary information due to privacy concerns. Data protection issues have hindered IP's ability to expand the NADB; most asset identification activity has depended on cooperation from states and federal agencies. The private sector has concerns that information provided for security purposes will expose them to competitive or legal scrutiny. Sectors with significant government oversight and national security concerns, such as nuclear and chemical industries, have been responsive to requests for data. Entities in other sectors such as business and finance, the defense industrial base, and telecommunications have been less forthcoming due to concerns about sensitive information, despite the creation of the Protected Critical Infrastructure Information (PCII) program.[41] Still other sectors such as emergency services and agriculture/food are highly distributed; different perspectives exist on how to best determine at-risk assets in a complex system. IP continues to seek, and license where necessary, data from numerous sources including its own institutional expertise, federal agencies, Industry Sector Advisory Councils, commercial entities selling data, and the private sector. IP is planning future data calls to states, and agencies are still in the process of identifying CI/KR.

Top 100 Lists. In May 2005, IP solicited each federal SSA for its most important CI/KR to create a consequence-driven dataset to help prioritize the NADB. Not all sectors have submitted responses. As of January 2006, three sectors (emergency services, information technology and agriculture/food) had not responded to IP's call for such a list. Furthermore, IP has integrated only five Top 100 lists into the NADB: three sectors (national monuments and icons, government facilities and postal and shipping), and two subsectors (drinking water and wastewater). IP has not finished processing responses for 10 other sectors. The submissions IP did receive varied in their utility. Some sectors have problems similar to those discussed above, including insufficient detail, information withheld due to security concerns, and a poor understanding of assets within a sector that cannot be reconciled with the NADB taxonomy. IP will continue to work with those sectors to ensure uniform and usable data as to the most important assets in each sector.

Gross Consequences of Attack. Led by a contractor., IP has been developing several complex methodologies for conducting a consequence-based analysis of a large number of targets. They are known as the Gross Consequences of

[41] The Protected Critical Infrastructure Information program solicits voluntary critical infrastructure information from proprietors by protecting such information from disclosure.

Attack (GCOA) tool.[42] This tool is an automated process for evaluating large numbers of targets and attack modes to estimate, at a high level, the consequences of terrorist attacks. IP intended to run the tool on the NADB in September 2005, but flaws in the methodology and data quality concerns stalled the development of the GCOA tool. These issues have now been resolved, but technical concerns continue to limit wide-scale implementation. At the time of our report, IP had not performed this analysis.

Expert Panels. IP intends to use expert panels consisting mostly of private sector representatives to review and refine the NADB. IP will provide panels data it has collected for each sector, including the results of gross consequence of attack analysis should it become available. The panels will focus on developing a methodology to measure and compare consequence by assigning values to various sector segments, such as prioritizing sector operations. The panels plan to review, sort, and rank all of their sector's assets, too. Delays in processing state-submitted data prevented the panels from convening last year. The first expert panel met for the chemical sector in March 2006, and IP intends for expert panels to have concluded for all sectors by October 2006.

Normalization. To develop a common risk analysis methodology that allows for comparability of consequence, vulnerability, threat and risk measurements, IP is developing a suite of tools called Risk Analysis and Management for Critical Asset Protection (RAMCAP). RAMCAP is intended to provide asset owners and operators a means to calculate the potential consequences and vulnerability to an attack using a common and consistent system of measurements, or the means to convert the results from prior assessments performed with select approved methodologies into results that can be compared to those obtained using RAMCAP methodologies. Without RAMCAP, the ability to gauge an individual asset's value or compare its importance to that of another asset will remain subjective and dependent upon the assessor's personal knowledge or awareness about an asset.

SSAs will complete and maintain their own risk assessments and IP will complete and maintain national cross-sector risk assessments. Risk assessments are ongoing and IP does not envision a definitive end-date when they will be complete. IP is working with the SSAs and other sector partners to develop, implement, and validate RAMCAP consequence and vulnerability assessment methodologies across the 17 CI/KR sectors. Assessments using RAMCAP have been conducted only in some sectors, in the pilot stages of

[42] The contractor developed three GCOA tools: Methodology for Indirect Economic Loss Model, Methodology for Casualty and Damage Models, and Hazard Methodology.

development in other sectors, and awaiting development in still other sectors. Individual proprietors in other sectors are using different assessment tools, and IP will need to determine whether it can incorporate the results of other assessment tools.

Interdependency Analysis. Understanding interdependencies is a key element in the future analysis and prioritization of CI/KR; the more IP understands interdependencies, the more it can confidently prioritize the NADB. As infrastructure by its nature has interconnected elements, the vulnerability of one asset may be dependent on another asset. These relationships require significant modeling and simulation to determine how cascading effects may create vulnerabilities. The National Infrastructure Simulation and Analysis Center (NISAC) is the government leader in the theoretical understanding of infrastructure interdependencies. IP coordinated in applying information from NISAC and other sources who are evaluating CI/KR. These entities have successfully modeled interdependencies in selected sectors independently of the NADB.

Recommendations

We recommend that the Under Secretary for Preparedness:

1. Define, and systematically examine, out-of-place or "extremely insignificant" assets, and determine which of those assets should remain in the NADB. Consider redesignating low-value assets remaining in the NADB.

2. Provide state homeland security advisors the opportunity to (a) review their previously submitted assets (with the taxonomy if necessary) that they believe fall within the definition of "extremely insignificant" and (b) recommend to DHS whether to retain them.

3. For ongoing and future data calls, clarify the guidance states should follow for what data to submit, and how DHS intends to use that data.

4. Identify and evaluate key milestones for the NADB and ensure that they are accurately captured in the NIPP.

Management Comments and OIG Analysis

DHS' Office of Preparedness commented on our draft report (a copy of its response in its entirety is recorded in Appendix B) and we incorporated several specific comments by DHS into this report. Additional analysis of DHS' comments and responses to the recommendations follows. Based on the response and additional discussions with NADB program officials, we modified each of our recommendations.

General Comments

Preparedness was concerned that the report did not accurately reflect the nature of criticality in the NADB, noting that the NADB is an inventory of assets across the nation to then be filtered to develop appropriate critical asset lists. It believes that criticality is not an important part of the initial inventory.

We understand the purpose of the inventory, but believe that considering the relevance of questionable data is worthwhile. We concur that criticality may be conditional, reflecting time or other concerns, and the NADB should include more than just assets of obvious criticality. For example, Preparedness suggested that schools are essential not for infrastructure protection, but for additional uses in operational support. While such ambitious uses of the NADB may be worthwhile, they should not distract from the stated mission of the NADB in supporting the protection of critical infrastructure. It should not be a reason to reject the concept of criticality, but rather a reason to refine the definitions of criticality applied. We have modified some of the language in the report to clarify the role of the NADB in the process of infrastructure protection.

Preparedness was also concerned that issues of insufficient staffing and funding were underrepresented in the report. We sought, and IP provided, some details regarding the NADB program budget. However, at the time of our report, we did not have sufficient information to draw conclusions regarding program needs. In its action plan to address Recommendation #4, IP should indicate whether funding shortfalls would impact its ability to meet certain milestones.

Specific Comment #8

Preparedness sought to clarify the role of the NADB as an asset inventory in the process of developing situational prioritized lists. Their response stated

that not only does the department not have one definitive prioritized list, but also that such a list is "neither possible nor useful…." Rather, Preparedness sees the NADB's mission as supporting "a variety of asset groups for programmatic focus or to answer specific questions."

We recognize the distinction between the NADB as an inventory and the multiple prioritized lists of CI/KR that are created using the inventory. We clarified this distinction in our final report. However, we maintain that a comprehensive picture of CI/KR across the entire nation's infrastructure is desired. The NIPP lists the "[p]rioritization of assets and systems across sectors and jurisdictions…"[43] as one of the stated goals of the next generation NADB. While the NADB is used to inform programmatic analyses, a maturing NADB is also essential to the development of a comprehensive picture of the nation's CI/KR.

While risk-based prioritization currently supports specific programs and sector-specific goals, it also has value in informing overarching budget priorities across CI/KR sectors. That said, we are not entirely clear as to what the "comprehensive picture"[44] will look like, and how DHS will interpret it to make funding decisions.

Recommendation #1: Define, and systematically examine, out-of-place or "extremely insignificant" assets, and determine which of those assets should remain in the NADB. Consider redesignating low value assets remaining in the NADB.

Preparedness perceived our original recommendation as misguided, representing a misunderstanding of the nature of the NADB's role as an inventory rather than as a critical list.

Based on Preparedness' response and discussions with program officials, we modified this recommendation. We believe that the presence of out-of-place assets still warrants management's attention. Over the development of this inventory, DHS has deferred to the judgment of the state, locality, or agency about which assets they should submit for the purposes of infrastructure protection, but there is evidence that these entities submitted assets for reasons other than state or local criticality assessments. This has led to out-of-place assets that should never have been included, and will never be used to inform

[43] Draft NIPP, p. 82
[44] Ibid

a risk assessment. Without a method to clean such assets from the inventory, time and money will be wasted to repeatedly filter out such assets for each analysis, and perhaps more importantly, their presence undercuts confidence in the inventory. Such out of place assets should be addressed.

IP already eliminates assets of "extreme insignificance," although criteria for identifying such assets have not been determined. Based on follow-up conversations with IP, most removed assets were removed because they were determined to not exist, but in rare instances, some assets were removed because they were deemed to have negligible value. This suggests that IP recognizes some value in eliminating out of place assets. We suggest that IP more clearly define assets of "extreme insignificance." This includes assets that are obviously out-of-place, as were many mentioned in this review.

Recommendation #1: Unresolved - Open

Recommendation #2: Provide state homeland security advisors the opportunity to (a) review their previously submitted assets (with the taxonomy if necessary) that they believe fall within the definition of "extremely insignificant" and (b) recommend to DHS whether to retain them.

Preparedness concurred with our recommendation. IP intends to provide assets maintained within the NADB to the respective states in the next data call to reduce duplicate submissions. States will also have the opportunity to identify assets that they believe not be included in the inventory.

Because IP will consider revising state assets in light of state concerns, we modified our recommendation to better reflect IP's plans. We agree that this information sharing may be productive in identifying assets that may not be relevant to the database, dependent on IP's assessment of the assets. It is unclear whether IP will give the same discretion to the state in removing assets as in submitting them. As part of its action plan, Preparedness should establish standards to guide the determination of assets.

Recommendation #2: Resolved - Open

Recommendation #3: For ongoing and future data calls, clarify the guidance given to states that discusses what data states should consider submitting, and how DHS intends to use that data.

Preparedness did not have the opportunity to respond specifically to this recommendation, which we developed through subsequent dialogue with NADB program officials. Program officials are developing improved guidance for the next data call.

As part of its action plan, Preparedness should provide an example of guidance for the next data call. This should include clarification of the purpose of the NADB and the intended breadth of assets to be contained within the NADB, to increase the consistency and comparability of state reports.

Recommendation #3: Resolved - Open

Recommendation #4: Identify and evaluate key milestones for the NADB and ensure that they are accurately captured in the NIPP.

Preparedness agreed with this recommendation in part. Preparedness raised an issue with the scope of our recommendation, as completion of a comprehensive risk analysis is not within the scope of the NADB. We agree that such an assessment is an activity that the NADB supports, and not an activity of the NADB program itself, and modified our recommendation accordingly. Preparedness is skeptical that it can produce a complete assessment, as the inventory and risk environment will continually evolve. Preparedness did agree on the importance of developing and refining clear milestones.

We agree that the on-going process will continue to develop key milestones. As part of its action plan, Preparedness should provide documentation of NADB milestones as they are incorporated into the NIPP. Preparedness should indicate whether funding shortfalls would impact its ability to meet certain milestones.

Recommendation #4: Resolved - Open

We reviewed the ongoing development of the NADB as a result of conclusions noted in our February 2004 survey report of what was formerly known within DHS as the IAIP directorate.[45] Our initial objective was to evaluate the effectiveness and efficiency of the processes used by IP to develop a prioritized list of the nation's critical infrastructure and assets. IP did not have a comprehensive, prioritized list but was actively collecting data from states to help create one. During 2005, we followed IP's progress toward completing the database. We also determined to what extent the database is supporting the NIPP and progressing toward a comprehensive, national risk assessment capability.

We assessed the methodology and results of DHS' 2004 data call to states for CI/KR information, as well as data DHS collected from states as part of the Office of Domestic Preparedness' State Self-Assessment Program.[46] We reviewed aggregate NADB data across multiple sectors and reviewed assets submitted by several states. We examined the NADB in July 2005 and again in January 2006. We reviewed documentation in support of the identification and selection process describing the business process. We became acquainted with IP's RAMCAP tool, as well as other agency-specific vulnerability and risk assessment activity.

We met with IP officials, including those managing the NADB program, and officials in other DHS components including the Transportation Security Administration and the United States Coast Guard. We visited homeland security officials in Florida, Illinois, Maryland, Massachusetts, Michigan, New Jersey, South Carolina, Texas, and Virginia. We interviewed representatives from the National Infrastructure Simulation and Analysis Center and the National Geospatial-Intelligence Agency. We also held meetings with representatives of the contractor that played a key role in processing the data submitted by states as part of the July 2004 data call.

We conducted our review between January 2005 and January 2006 under the authority of the *Inspector General Act of 1978*, as amended, and according to

[45] "Survey of the Information Analysis and Infrastructure Protection Directorate," OIG-04-13, February 2004, p.24.
[46] In 2003, states and urban areas participated in an assessment process that reflected post-9/11 threats and vulnerabilities. This second process enabled states and urban areas to refine and further develop their Homeland Security Strategies.

the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency.

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

Homeland Security

April 13, 2006

MEMORANDUM TO: Robert L. Ashbaugh
Assistant Inspector General for Inspections
and Special Reviews

FROM: George W. Foresman
Under Secretary

SUBJECT: *Response to Draft Inspector General Report on the Progress in Developing the National Asset Database*

This responds to the March 8, 2006, memorandum requesting the Directorate for Preparedness' comments on the draft Office of the Inspector General report, *Progress in Developing the National Asset Database*. First, we sincerely appreciate the opportunity to respond to the draft report. The attached document provides comments on the 4 recommendations directed to Preparedness. In addition, we are providing some additional comments to clarify the National Asset Database Program described in the report. Questions concerning specific comments should be addressed to Joshua Burleigh at 202-282-8547.

Please accept our thanks for the opportunity to respond to the draft report and to work with the Office of the Inspector General during this engagement. As Preparedness works toward refining its programs, the Office of the Inspector General's independent analysis of program performance greatly benefits our ability to continuously improve our activities. We look forward to continuing this partnership in the future.

Attachment

cc: Robert Stephan
Steven Pecinovsky

Response to recommendations contained in the Draft OIG Report
Developing the National Asset Database

General Comments

1) The first point of clarification is that the National Asset Database (NADB) is not a list of critical assets assembled into a database of only those assets (facilities, systems and infrastructures) deemed "critical." The NADB is the primary Federal data repository for analysis and integration required to provide the Department of Homeland Security (DHS) with the capability to identify, collect, catalog, and maintain a *national asset inventory*. This misperception is interwoven throughout the document and should be clarified in order to reduce further dissemination of unclear or misperceived programmatic focus for the NADB. The NADB is a continually evolving and comprehensive catalog of the assets that comprise the Nation's infrastructure; containing descriptive information regarding those assets. Since the NADB is an inventory of assets, it can be queried in many ways that can help inform public and private risk-reduction activities across the 17 Critical Infrastructures and Key Resources (CI/KR) sectors. It provides the "universe" from which various lists of critical assets are produced. The NADB enables a wide-ranging robust risk analysis process that ties asset information, as well as analyses concerning consequence of loss/attack, vulnerability of an asset, system or network, to the threat to those assets, systems, or networks. Artificial limits on the scope of the database will prevent a complete risk analysis. Many assets not "critical" are, in fact, critical depending upon the circumstances including timing, the nature of an event, interdependencies, etc. Additionally, the ongoing interdependency analysis identifies components that are important due their linkage or support to other assets or systems.

The third paragraph in the Executive Summary of the draft report states that the "while the NADB includes many vital assets easily recognizable as critical, it also includes assets that do not appear, and IP does not necessarily interpret, to meet criticality requirements promulgated by DHS." It further states that due to these assets which do not meet a level of criticality, "the current NADB is tainted enough to question whether it is an accurate representation of the nation's CI/KR." This is just one indication that the authors of this portion of the report have missed the fundamental purpose and nature of the NADB. The data in the NADB have been and are currently being utilized to support allocation decision making processes for the Department. The process also continues to mature and improve.

In comparison to the above misperception, page 5 correctly outlines the actual intent of the NADB as a "comprehensive catalog that includes an inventory and descriptive information regarding the assets and systems that comprise the nation's CI/KR." Though there are multiple interpretations of the term 'CI/KR', that previous statement could be accurately perceived that the NADB encompasses infrastructure information regarding assets/systems across all 17 infrastructure sectors.

2) A topic that is underrepresented is the impact that insufficient manning and funding of the program has had on progress. Additional details to effectively represent this topic are

being provided through the ongoing monthly investigative sessions with the Inspector General. Determination of the final delivery of the report has not yet been made.

Response to recommendations Contained in the Draft OIG Report
Developing the National Asset Database

Specific Comments

1. Page 6: Liberty Shield List contained 160 assets; not the 145 listed.
2. Page 7, Footnote 19: The classified NADB production system is housed and maintained at .
3. Page 9, Footnote 20: The classified NADB production system is housed and maintained at .
4. Page 10: The taxonomy is a methodology for classifying the national infrastructure into it proper areas. The report mischaracterizes it as a risk analysis methodology. Additionally, the taxonomy currently being used to structure the NADB and has been shared with our partnering Sector Specific Agencies (SSAs) as well as other entities that have data the Department is seeking to access or collect.
5. Page 11: The Department has not characterized any data in the current NADB as useless. Risk Management Division (RMD) is also aware that some states submitted assets that were designated by states as critical to them, but that did not meet the criteria for "assets of national importance." The Department specifically did not exclude these important state assets because it is building a catalogue of assets, and in order to fully partner with the state and local governments, the Department must be informed about what is important to the state and local entities to properly work together and target resources to the areas of greatest concern.
6. Page 12: The NADB taxonomy is the first step in delineating and creating a consistent approach to the listing of assets, systems and networks across the SSAs and down to the local level.
7. Page 12: The poor quality of the 2003 Office of Domestic Preparedness (ODP) data call was one of the reasons the Department has spent time and resources verifying that data and ensuring future efforts to collect data were properly planned.
8. Page 17: It is true the Department does not have one definitive prioritized list of CI/KR. Such a definitive list is neither possible nor useful, and is not an objective of DHS. Rather the **ability** to **produce** prioritized lists of critical infrastructure based upon a **need** or a **situation** is the ability embodied by the NADB and the risk analysis capability that accompanies it. The NADB though is crucial to being able to provide a variety of asset groups for programmatic focus or to answer specific questions. The NADB is being developed to answer those many types of questions depending on the threat or the risk and has been called upon in areas as diverse as terrorism and hurricane preparations.
9. Page 19: The NADB assets were considered and utilized to support the grant decision making process. In some cases, additional information was sought to assist in the grant process, but that was to add to the base of information needed for the grant process as the NADB continues to mature. It was not a question of accuracy, but richness of data that the Department is working to deepen.

10. Page 20: The Emergency Services sector, not Energy, has not yet submitted specific assets in regard to the Department's Top 100 request.
11. Page 20: A point made in the report that was not emphasized enough was the issues surrounding data protection. "Data protection issues have hindered IP's ability to expand the NADB; most asset identification activity has depended on cooperation from states and federal agencies." Asset owners and operators have the most accurate and detailed information desired to conduct adequate analysis, yet industry is reluctant to provide the information due to fears of a lack of clear and complete data protection capabilities. The NADB system exceeds all security and protection standards and will handle the information as classified and/or designated by the source or under current guidance, but without sufficient legal justification and legislation, further protection is currently unavailable.
12. Page 21: The deployment of the Gross Consequences of Attack Tool was due to incorporation of the geospatial solution and IT integration issues. These have been resolved and the tool will be operational in April 2006.
13. Page 21: Expert panels are currently being utilized to refine the NADB. The first panel for the Chemical Sector met in March 2006, the panel for Emergency Services will meet in April 2006. All proposed expert panels for the sectors will have met by September 2006.
14. Page 22: The DHS National Infrastructure Simulation and Analysis Center (NISAC) is the lead DHS entity for interdependency analysis. It has been provided and utilized the NADB taxonomy and asset information in the NADB. Stood up in 2000, it had a jump on data acquisition. The experts at NISAC are collaborating with the NADB team to facilitate the future exchange of information between the two entities with will be greatly increase as the issues of data licensing and propriety are resolved.

Response to recommendations Contained in the Draft OIG Report
Developing the National Asset Database

Recommendations

Recommendation #1: Review the National Asset Database (NADB) for out-of-place assets and assets marked as not nationally significant, and determine whether those assets should remain in the NADB. The review should encompass how it is categorizing these assets and consider re-designating them.

Response: Preparedness non-concurs. Recommendation #1 is guided by the misperception that the NADB is merely a critical asset list. During the verification process, assets that are determined to have closed, moved, or been of extreme insignificance are removed. However, assets that may not be 'critical', yet are a part of the nation's infrastructure, are still maintained in the database. An accurate example used within the report (page 11) that represents an infrastructure to be maintained in the NADB that is not 'critical' includes local schools. Individual schools may not be considered of national significance or of 'criticality' when compared to a nuclear facility or chemical manufacturing plant, but infrastructure information on schools would be highly beneficial in determining evacuation facilities or possible areas for improvised patient collection in response to major incidents or natural disasters. Additionally, the term "National" is used to show national coverage in length and depth, as opposed to the "Federal" asset database.

Recommendation #2: Provide state homeland security advisors the opportunity to review their assets in the NADB (with the taxonomy) to identify previously submitted assets that may not be relevant.

AND

Recommendation #3: During future data calls, provide States a list of their respective NADB assets to reduce the likelihood of duplicate submissions.

Response: Preparedness concurs. Recommendations #2 and #3 are valid recommendations planned to be resolved in the next data call to the States and Territories. It is expected that the assets maintained within the NADB will be provided to the respective localities to supply the updated information and facilitate information exchange. This also provides awareness of which of the States' assets are included in the national dataset so that the State can submit only those additional assets that they have that are not currently included in the NADB. The report accurately outlines the deficiencies with the July 2004 data call and some of the inaccurate data that resulted. Assets in many cases were vague and incomplete, requiring a large-scale verification and validation effort to ensure the data that is currently included in the NADB is more complete, accurate, and relevant. But it should also be noted that assets in the NADB

have been previously provided to the states and the new generation NADB will all open access to the state for its assets, security protocols withstanding.

Recommendation #4: Establish a milestone for the completion of a comprehensive risk assessment of CI/KR. Identify and evaluate key milestones for the NADB and ensure that they are accurately captured in the NIPP.

Response: Preparedness generally concurs. Recommendation #4: Additional milestones for the NADB continue to be developed and refined. However, a milestone for the completion of a comprehensive risk assessment is not representative or within the scope of the NADB. The NADB is a continually evolving repository of information and will therefore never be 'complete.' Regarding comprehensive risk assessments, the NADB is the catalog of information that should feed risk analysis- not the tool through which risk analysis is executed. Milestones and metrics should therefore represent the infrastructure information identification, collection, and dissemination. An ongoing risk analysis of assets, systems and networks contained within the NADB is ongoing now and is envisioned to continue, expand and be as comprehensive as achievable.

Roles and Responsibilities within NIPP Risk Management Framework

Notes: **X** = Required action **O** = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
2	**AUTHORITIES, ROLES, AND RESPONSIBILITIES**										
	Complete SSP development.		+			X					
	Submit Annual CI/KR Protection Reports to DHS.				Jul 1	X	X	X	O	O	
	Complete National NIPP Funding Report.				Sep 1	X					
	Review and revise CI/KR-related plans as needed to align them with the NIPP.		+			X	X	X			
	Review and revise homeland security program and associated plans as needed to align them with the NIPP.			+					O	O	O
3	**THE PROTECTION PROGRAM STRATEGY: REDUCING RISK**										
3.1	**Set Security Goals**										
	Develop and update the national risk profile in collaboration with security partners.			+		X					
	Establish sector security goals that support NIPP goals and objectives.		+				X				
3.2	**Identify Assets**										
	Identify desired information by asset type and develop sector inventory guidance.	+				X	X	X	O	O	O
	Develop tools and methodologies to assist security partners in identifying cyber assets.		+			X					
3.3	**Assess Risks**										
3.3.1	***Baseline Criteria for Assessment Methodologies***										
	Review existing risk assessments or methodologies used to assess compatibility with the DHS baseline criteria. "Translate" the results or adjust the methodology if they differ from the baseline criteria.		+			X	X				
	Assist the SSAs and other security partners to determine the common criteria for risk assessments.		+			X					
3.3.2	***Consequence Analysis***										
	Provide a timeline for the development of sector-specific methodologies including RAMCAP modules and for conducting consequence-based top screening for all CI/KR sectors.	+				X	X				
	Define common terminology and metrics for use in assessing consequences.		+			X					
	Conduct consequence-based top screening for first priority CI/KR sectors.		+			X	X		O	O	O
	Work with security partners to develop consequence assessment methodologies for the first priority CI/KR sectors with completed top screening.		+			X	X				
	Conduct consequence assessments at CI/KR assets with potentially high consequences for the first priority CI/KR sectors based on the results of the top-screening process.		+			X	X		O	O	O

Notes: X = Required action O = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
3.3.3	***Vulnerability Assessment***										
	Work with DHS to validate the results of assessments for sector assets that are of the greatest concern and involve owners and operators in the review whenever possible.	+					X			O	O
	Develop sector-specific vulnerability assessment methodologies (e.g. RAMCAP Vulnerability Assessment modules) for the first priority CI/KR sectors.		+			X	X				
	Conduct vulnerability assessments for CI/KR assets in the first priority sectors and identify common cross-sectors vulnerabilities.		+			X	X		O	O	O
3.3.4	***Threat Analysis***										
	Develop first quarterly sector-specific CI/KR threat assessment.	+				X					
	Identify intelligence collection requirements.			+		X		X			
3.4	**Prioritize**										
	Use analysis-based normalization tools to convert risk assessment results (analyses that do not meet the NIPP baseline criteria) into measures that can be used for national-level comparison.		+			X			O		
	Prioritize CI/KR protection needs based on normalized scores from risk assessments.		+			X			O		
3.5	**Implement Protective Programs**										
	Identify gaps in protection for high priority CI/KR.				Jul 1	X	X		O		
	Review current protective programs in relationship to identified gaps.				Jul 1	X	X		O		
	Augment existing programs, or design and implement new protective programs for the remaining gaps.				Sep 1	X	X		O	O	
3.6	**Measure Effectiveness**										
3.6.1	***NIPP Metrics and Measures***										
	Provide guidance on metrics for annual reporting and national-level, cross-sector comparative analysis.		+			X					
3.6.2	***Gathering Performance Information***										
	Gather information needed to measure performance associated with each set of core and sector-specific metrics.			+		X					
3.6.3	***Assessing Performance and Reporting on Progress***										
	Use risk assessment information to develop Annual Reports to the Secretary of Homeland Security.				Jul 1		X				
	Use risk assessment to inform Annual Reports to DHS on State CI/KR protection program.				Jul 1				O		
3.7	**Continuous Improvement**										
	Use national-level risk assessment to generate a cross-sector report that describes national progress toward CI/KR protection goals and needed improvements.				Sep 1	X					

Notes: **X** = Required action **O** = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
4	**ORGANIZING AND PARTNERING FOR CI/KR PROTECTION**										
4.1	**Leadership and Coordination Mechanisms**										
	Commence SSC and GCC operations.	+				X	X		O	O	O
	Establish a point of contact within DHS for national-level NIPP coordination with regional entities.	+				X					
	Implement mechanisms to enable selected regional entities to access the sector partnership model at the national level.		+			X	X				
	Review established coordination mechanisms to ensure that they accommodate NIPP requirements.			+					O	O	O
4.2	**The Information-Sharing Strategy: A Networked Approach**										
	The Homeland Security Information Network										
	Implement sector-specific policies and protocols for vetting and disseminating routine information to owners and operators.	+				X	X				
	Complete rollout of HSIN-CS to all sectors.			+		X					
	Work with security partners to measure the efficacy of the HSIN and identify requirements for new mechanisms or supporting technologies.			+		X	X	X	O	O	O
	Lessons Learned and Best Practices										
	Ensure that the NIMS Integration Center includes information on CI/KR protection best practices.	+				X	X				
4.3	**Protection of Sensitive CI/KR Information**										
	Review information protection practices to ensure they comply with the Interim PCII Rule and the Final Rule when published.		+			X					
5	**INTEGRATING CI/KR PROTECTION AS PART OF THE HOMELAND SECURITY MISSION**										
5.3	**Relationship of the NIPP to Other CI/KR Protection Plans and Programs**										
5.3.1	***Sector-Specific Plans***										
	Coordinate SSP planning with security partners, including completion of a review and concurrence process.		+				X				
	Review NIPP Base Plan and establish program management processes needed to support plan implementation within each sector.	+					X				
	Coordinate with the SSAs to provide guidance and support for SSP development.		+			X					
	Review SSPs to verify that cross-sector requirements have been identified.			+		X					
5.3.2	***State, Regional, Local, and Tribal CI/KR Protection Programs***										
	Review, revise, or develop homeland security program and associated plans as needed to ensure seamless linkage between the NIPP steady-state CI/KR protection and incident management activities.			+					O	O	
5.3.3	***Other Security Partner Plans or Programs Related to CI/KR Protection***										
	Review and revise CI/KR-related plans as needed to ensure seamless linkage between the NIPP steady-state		+			X	X	X			

Notes: X = Required action O = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
	CI/KR protection and incident management activities.										
	Review and revise homeland security program and associated plans as needed to ensure seamless linkage between the NIPP steady-state CI/KR protection and incident management activities.			+					O	O	O
5.4	**CI/KR Protection and Incident Management**										
	Review current Federal CI/KR protection measures to ensure alignment with the HSAS threat levels.		+			X	X	X			
	Review current State, local, tribal, and private sector CI/KR protection measures to ensure that they align with the HSAS threat levels.			+					O	O	O
	Develop written procedures to ensure seamless transition from steady-state CI/KR protection to activities required to inform and enable incident management decisions and activities.			+			X	X	O	O	O
6	**ENSURING AN EFFECTIVE, EFFICIENT PROGRAM OVER THE LONG TERM**										
6.1	**Building National Awareness**										
	Identify and assess the requirements for a national CI/KR protection awareness program.	+				X					
	Convene an interagency national CI/KR public awareness workgroup.	+				X					
	Conduct an inventory of existing national public awareness efforts or partnerships that could support the delivery of CI/KR protection messages to broad audiences.		+			X					
	Develop and implement a comprehensive national CI/KR protection awareness program.			+		X	X	X	O	O	O
	Conduct initial CI/KR protection public awareness activities called for under the national awareness plan within the State, local, and tribal jurisdictions.			+					O	O	
6.2	**Enabling Education, Training, and Exercise Programs**										
6.2.2	***Education and Training***										
	Review training programs to ensure that they are consistent with NIPP requirements.	+				X	X	X	O	O	O
	Provide the initial training on the NIPP to introduce all security partners to the Plan's contents and requirements.		+			X					
	Make recommendations for training program revision to conform to NIPP requirements.		+			X	X	X	O	O	O
	Revise training programs to conform to NIPP requirements.			+		X	X	X	O	O	O
6.2.3	***Organizational Training and Exercise Programs***										
	Ensure that DHS exercises include adequate testing of steady-state CI/KR protection measures and plans.			+		X					
	Ensure that DHS exercises include tests of the interaction between the NIPP framework and the NRP incident management framework.			+		X					
	Ensure that DHS exercises include a focus on CI/KR interdependencies and protection collaboration across			+		X					

Notes: X = Required action O = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
	jurisdictional and sector boundaries.										
6.3	**Conducting Research and Development**										
	Gather information on industry advances in CI/KR protection-related science and technology; ensure that these are periodically reviewed by the NSTC.		+			X	X	X			O
	Convene discussions and workshops with security partners to determine CI/KR R&D priorities.		+			X			O	O	O
	Share sector-specific threat handbooks with the CI/KR R&D communities to guide emphasis and timing of future R&D activities.		+			X	X	X			
	Identify and communicate to DHS requirements for CI/KR-related R&D for use in the national R&D planning effort.			+		X	X	X	O	O	O
	Develop a comprehensive database to manage Federal R&D investments related to CI/KR protection.			+		X	X	X			
	Work with OSTP to establish an updating cycle for the annual NCIP R&D Plan; update plan according to cycle.			+		X					
	Work with OSTP to incorporate sector-level R&D requirements into the updating of the NCIP R&D Plan.			+		X					
6.4	**Building and Maintaining Databases, Simulations, and Other Tools**										
6.4.1	***National CI/KR Protection Data Systems***										
	Establish appropriate data-collection formats for national infrastructure inventory.		+			X					
	Identify all databases containing information useful to CI/KR protection and national inventory.			+		X	X	X			
6.4.2	***Simulation and Modeling***										
	Establish requirements for the development, maintenance, and use of research- and operations-related modeling capabilities for CI/KR protection.		+			X					
	Review existing private sector modeling initiatives and opportunities for joint ventures to ensure that DHS and its security partners make maximum use of private sector modeling capabilities.			+		X					O
	Review existing SSA modeling capabilities for potential use in CI/KR protection.			+		X	X				
6.4.3	***Coordination With Security Partners on Databases and Modeling***										
	Specify the timelines and milestones for the initial population of asset databases.	+				X					
	Specify a regular schedule for maintenance and updating of databases.	+				X					
	Identify databases and other data services that can be used to populate asset databases.			+		X	X	X	O	O	O
	Outline sector plans and processes for the development and updating of databases, data systems, modeling, and simulation.			+			X				
6.5	**Continuously Improving the NIPP and SSPs**										
	Establish the mechanism(s) necessary to coordinate SSP review and maintenance.		+				X				

Notes: **X** = Required action **O** = Recommended or encouraged action

Chapter and Section		Milestone				Security Partner					
		90 Days After NIPP Approval	180 Days	365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal	State or Territory	Local and Tribal	Private Sector
	Conduct first annual review of the NIPP and SSPs to identify changes that warrant the issuance of a periodic update (e.g., new laws, orders, procedures, etc.).			+		X					
7	PROVIDING RESOURCES FOR THE CI/KR PROTECTION PROGRAM										
7.1	The Risk-Based Resource Allocation Process										
	Work with SSAs and the States to develop a national cross-sector picture of funding sources for CI/KR protection.	+				X	X	X	O		
	Work with the SSAs and the States to address funding gaps or duplicative efforts identified through the budget coordination.				Jul 1	X	X		O		
	Use information gathered from the SSAs and the States to assess cross-sector CI/KR protection efforts, progress, funding, and outstanding needs as the basis for the NIPP National Funding Report.				Sep 1	X	X		O		
	Work with respective department or agency budget process to identify and develop NIPP-related aspects of their annual budget submissions.				Sep 1	X	X	X	O	O	
7.2	Federal Resource Allocation Process for DHS, SSAs, and Other Federal Agencies										
	Coordinate Annual Report development with sector security partners, SCCs and GCCs to identify existing sector-specific CI/KR protection programs, NIPP-related initiatives, priorities, R&D funding and S&T investment requirements, critical gaps, and funding projections.				Jul 1	X	X	X	O	O	
	Develop and submit to OMB the National NIPP Funding Report that summarizes NIPP-related investment recommendations, identifies NIPP requirements, and summarizes NIPP funding requests across sectors and States.				Sep 1	X					
7.3	Federal Resources for State and Local Government Preparedness										
	Ensure annual homeland security grant guidance includes adequate consideration of CI/KR protection priorities.	+				X					
	Identify potential funding sources for State CI/KR protection efforts.		+				X				
	Develop guidance for State, Territorial, and tribal CI/KR protection programs to ensure they are aligned with grant application requirements.				as req	X					
	Work through the State Administrative Agencies to identify and prioritize the homeland security needs identified in State Homeland Security Strategies and Program and Capability Enhancement Plans, and identify assistance from all funding sources that may address these needs.				as req	X			O		
	Apply for homeland security grants to address CI/KR protection efforts per DHS/G&T guidance.				as req				O	O	

Critical Infrastructure and Key Resource Sectors

- Agriculture and Food
  - Supply Processing/ Packaging/Production
  - Agricultural and Food Product Storage
  - Agricultural and Food Production Transportation
  - Agricultural and Food Production Distribution
  - Agricultural and Food Production Facilities
  - Regulatory, Oversight, and Industry Organizations
  - Other Agriculture and Food
- Banking and Finance
  - Banking and Credit
  - Securities, Commodities, and Financial Investments
  - Insurance Carriers
- Chemical and Hazardous Materials Industry
  - Chemical Manufacturing Plants
  - Hazardous Chemical Transport
  - Hazardous Chemical Storage/Stockpile/Utilization/Distribution
  - Regulatory, Oversight, and Industry Organizations
  - Other Hazardous Chemical Facilities
- Defense Industrial Base
  - Shipbuilding Industry
  - Aircraft Industry
  - Missile Industry
  - Space Industry
  - Combat Vehicle Industry
  - Ammunition Industry
  - Weapons Industry
  - Troop Support Industry
  - Information Technology Industry
  - Electronics Industry
  - Electrical Industry Commodities
  - Mechanical Industry Commodities
  - Structural Industry Commodities
- Energy
  - Electricity
  - Petroleum
  - Natural Gas
  - Regulatory, Oversight, and Industry Organizations
- Emergency Services
  - Law Enforcement
  - Fire, Rescue, and Emergency Services
  - Search and Rescue
  - Emergency Medical Services
  - Emergency Management
  - Other Emergency Services
- Information Technology
  - Hardware Production
  - Software Production
  - Information Technology Services
  - Internet
  - Next Generation Networks
  - Regulatory, Oversight, and Industry Organizations
  - Other Information Technology Facilities
- Telecommunications
  - Wired Telecommunications
  - Wireless Telecommunications
  - Satellite Telecommunications
  - Internet
  - Next Generation Networks
  - Regulatory, Oversight, and Industry Organizations
  - Other Telecommunications Facilities
- Postal and Shipping
  - U.S. Postal Service
  - Couriers
  - Other Postal and Shipping Facilities
- Healthcare and Public Health
  - Direct Patient Healthcare
  - Public Health Agencies
  - Healthcare Educational Facilities
  - Health Supporting Facilities
  - End-of-Life Facilities
  - Regulatory, Oversight, and Industry Organizations
  - Other Healthcare and Public Health Facilities
- Transportation
  - Aviation
  - Railroad
  - Road
  - Maritime
  - Mass Transit
  - Pipelines
  - Regulatory, Oversight, and Industry Organizations
- Water
  - Raw Water Supply
  - Raw Water Transportation
  - Raw Water Storage
  - Water Treatment Facilities
  - Treated (Finished) Water Storage
  - Treated Water Distribution Systems
  - Treated Water Monitoring Systems
  - Treated Water Distribution Control Centers
  - Wastewater Facilities
  - Regulatory, Oversight, and Industry Organizations
- National Monuments and Icons
  - National Monument/Icon Structures
  - National Monument/Icon Geographic Areas
  - National Monument/Icon Documents and Objects
  - Other National Monuments and Icons
- Commercial Assets
  - Business Assets
  - Community Assets
  - Industrial Assets
  - Other Commercial Assets
- Government Facilities
  - Executive Branch Facilities
  - Legislative Branch Facilities
  - Judicial Buildings
  - Foreign Government Buildings
  - Other Government Facilities
- Dams
  - Low Hazard Potential Dams
  - Significant Hazard Potential Dams
  - High Hazard Potential Dams
  - Regulatory, Oversight, and Industry Organizations
- Nuclear Facilities
  - Nuclear Power Plants
  - Research, Training, and Test Reactors
  - Nuclear Fuel Cycle Facilities
  - Radioactive Waste Management
  - Nuclear Materials Transport
  - Deactivated Nuclear Facilities
  - Radioactive Material Users
  - Radioactive Source Production and Distribution Facilities
  - Regulatory, Oversight, and Industry Organizations
  - Other Nuclear Facilities

On July 19, 2004, the Assistant Secretary, Office of Infrastructure Protection, sent to State/Territorial Homeland Security Advisors via memorandum the following guidelines:

Guidelines for Identifying National Level Critical Infrastructure and Key Resources

CRITICAL INFRASTRUCTURE

AGRICULTURE/FOOD

1. Distribution facilities that ship to 5 or more states.
2. Food Processors with product distribution to more then 10 states.
3. Producers with herd of more then 20,000 Bovine, 30,000 swine or 500,000 poultry or distribution to more then 10 states or production of 50,001-250,000 bushels of crops.

BANKING & FINANCE

1. Wholesale Securities/Funds Transfer Services in excess of $50B per year.
2. Financial entities that provide wholesale funds or government securities transfer and settlement services.
3. Primary dealers in the government securities market.
4. Primary/Backup for the backbone computer infrastructure for stock market exchanges
5. Major banking and financial centers.

CHEMICAL

1. Sites that could cause death or serious injury in the event of a chemical release and have greater than 300,000 persons within a 25-mile radius of the facility.
2. Economic impact of more than one billion dollars per day (e.g., an event impacting multiple sectors and cumulatively cause this amount of economic damage).

NOTE: The term “sites” includes manufacturing plants; rail, maritime, or other transport systems; pipeline and other distribution networks; and storage, stockpile, and supply areas.

ENERGY (EXCEPT NUCLEAR POWER)

Electricity

1. Major power generation facilities that exceed 2000MW and if successfully attacked would disrupt the regional electric grid.
2. Hydroelectric facilities and dams that produce power in excess of 2000MW or could result in catastrophic loss of life if breached.
3. Substations that are the **sole-source** of power to critical commercial or government facilities

4. Regional transmission coordination centers: Control centers for Regional Transmission Organizations, Independent Transmission Operators, and Regional Coordinators.
5. Transmission substations necessary for the reliable operation of the transmission grids
6. Electric substations 500Kv or larger, and substations 345Kv or larger that are part of a critical system supporting population in excess of one million people.

Oil & Gas

1. Refineries with refining capacity in excess of 225,000 barrels per day.
2. Product pipelines with a capacity in excess of 200,000 barrels per day.
3. Natural gas pipelines with a capacity equal to or greater than 1 billion cubic feet per day.
4. Natural Gas and liquid Natural Gas Storage (LNG) facilities.
5. Major petroleum handling facilities such as pipelines, ports, refineries and terminals.

EMERGENCY SERVICES

1. National Emergency Operations Centers (e.g. HSOC, NICC, NRC, USCOE, etc.)
2. Operation centers responsible for receiving and disbursing National Strategic Stockpile Supplies at the state level, and in support of urban center distributions with populations greater than one million.

INFORMATION TECHNOLOGY

1. IT Systems: Systems with access or control points distributed on both coasts and throughout the country.
2. Networks: Networks with nodes distributed on both coasts and throughout the country.
3. Digital Control Systems: Control Systems with access or control points distributed on both coasts and throughout the country.
4. Major Primary data storage and processing facilities.

TELECOMMUNICATIONS

1. Major telephony hotels.
2. Control centers controlling national or regional telephonic traffic.

POSTAL & SHIPPING

1. Major collection, sorting or distribution centers for national or regional shipments.

PUBLIC HEALTH

1. Primary medical care facilities with unique services (i.e. shock trauma units) serving populations of greater than 250 thousand.
2. Primary blood supply facilities servicing national and regional areas.
3. National Stockpile and unique pharmaceutical (i.e. vaccine facilities for flu, small pox) facilities.

TRANSPORTATION

Rail (Freight):

1. Railroad Information Technology and Communications Infrastructure critical nodes.
2. Rail tunnels and bridges or other critical assets where no practical reroute and rebuild time is over six months if all resources are available, rerouting results in 75% degradation of service.
3. Primary entry points used to transport commercial or military shipments, which if destroyed would significantly impact the people, economy or national security.
4. Unsecured rail yards, located within populated areas (greater than 50K), that on any given day, contain large quantities (greater than 5 tank cars) of poison inhalation hazard materials.
5. Rail yards that if disabled would cause significant disruption of national economy.

Mass Transit (Main/Major Terminals—Subways/Bus/Rail/Cruise)

1. Subways: Subway systems and supporting ventilation systems.
2. Bus: Terminals located within urban centers with a population of greater than 500K or servicing >5K passengers daily.
3. Passenger Rail: Terminals located within urban centers with a population of greater than 500K or servicing greater than 50K passengers daily.
4. Cruise: Ports/Terminals located within urban centers with a population of greater than 500K or servicing greater than 10K passengers daily.

Maritime

1. Seaports that have been designated Strategic National Defense Seaports.
2. Seaports that represent the majority of imports and exports of containerized and petroleum cargoes.
3. Seaports and facilities that service the Strategic Petroleum Reserve.
4. Locks & dams critical for the operation of major inland commercial waterways.
5. Harbor entrance waterway choke points that if blocked would deny port access.

Aviation

1. Major airports (passenger and freight).

WATER

Supply

1. Water treatment facilities, ground water systems (wells), water transmission systems (aqueducts, viaducts, pipelines, open channel) that serve populations or water reservoir system(s) including ground or elevated that serve populations of greater that one million persons.

Wastewater

1. Waste water treatment facilities, wastewater collection systems and pumping systems (force mains) or wastewater storage system(s) that serve populations greater than one million persons.

NATIONAL MONUMENTS & ICONS

1. Monuments/icons of national significance.

Key Resources

COMMERCIAL FACILITIES

1. **Commercial Centers:** Loss creates economic impact of greater than $10 billion or has a capacity greater than 35,000 individuals
2. **Office Buildings**
    a. Height greater than 500 feet and/or of significant importance.
    b. Economic impact of loss greater than $10 billion
    c. Capacity greater than 8,000 individuals
3. **Stadiums – Arenas:** Economic impact of loss greater than $10 billion or capacity greater than 25,000 individuals
4. **Amusement/Theme Parks:** Economic impact of loss greater than $10 billion or capacity greater than 35,000 individuals
5. **Public Institutions (Educational Facilities):** Economic impact of loss greater than $10 billion or capacity greater than 25,000 individuals
6. **Hospitality Industry:** Economic impact of loss more than $10 billion or capacity more than 8,000 individuals

GOVERNMENT FACILITIES

1. Federal or state-level COOP/COG facilities

DAMS

1. High hazard dams, or dams that produce over .5 megawatts of hydropower or provide irrigation to agriculture greater than 10,000 acres or provide for navigation on significant waterways or provide flood control or locks that provide significant waterway navigational ability or levees that provide significant flood control that the loss of which would cause significant economic impact or loss of life.

NUCLEAR REACTORS AND SPENT FUEL FACILITIES

Critical Infrastructure/Key Resource Totals by State

	State or Territory	Number of Assets already on NADB (FY04)	Number of Assets submitted on NADB (FY05)	Number of Assets on the NADB (FY04) and the NADB (FY05) (Duplicates)	Percentage of NADB (FY05) Assets submitted that were duplicates of the NADB (FY04) Assets	Number of New Assets resulting from the NADB (FY05) Data Call	Total Number of Assets in the Database
1	Alabama	701	39	30	76.92%	9	710
2	Alaska	552	87	4	4.60%	83	635
3	American Samoa	-	-	-	-	-	10
4	Arizona	597	151	73	48.34%	78	675
5	Arkansas	367	144	15	10.42%	129	496
6	California	3122	737	647	87.79%	90	3212
7	Colorado	422	872	1	0.11%	871	1293
8	Commonwealth of Northern Marianas	-	-	-	-	-	28
9	Commonwealth of Puerto Rico	97	33	-	-	33	130
10	Connecticut	465	578	113	19.55%	465	930
11	Delaware	51	415	11	2.65%	404	455
12	District of Columbia	308	158	50	31.65%	108	416
13	Florida	1453	688	127	18.46%	561	2014
14	Georgia	1493	74	53	71.62%	21	1514
15	Guam	-	-	-	-	-	116
16	Hawaii	92	116	6	5.17%	110	202
17	Idaho	153	595	1	0.17%	594	747
18	Illinois	1801	429	171	39.86%	258	2059
19	Indiana	322	8303	34	0.41%	8269	8591
20	Iowa	349	147	41	27.89%	106	455
21	Kansas	631	694	342	49.28%	352	983
22	Kentucky	774	397	48	12.09%	349	1123
23	Louisiana	447	393	94	23.92%	299	746
24	Maine	208	80	17	21.25%	63	271
25	Maryland	591	1152	51	4.43%	1101	1692
26	Massachusetts	339	477	52	10.90%	425	764
27	Michigan	916	631	80	12.68%	551	1467
28	Minnesota	548	65	36	55.38%	29	577
29	Mississippi	948	100	22	22.00%	78	1026
30	Missouri	448	261	25	9.58%	236	684
31	Montana	248	1148	11	0.96%	1137	1385
32	Nebraska	1389	2401	333	13.87%	2068	3457
33	Nevada	468	157	18	11.46%	139	607

	State or Territory	Number of Assets already on NADB (FY04)	Number of Assets submitted on NADB (FY05)	Number of Assets on the NADB (FY04) and the NADB (FY05) (Duplicates)	Percentage of NADB (FY05) Assets submitted that were duplicates of the NADB (FY04) Assets	Number of New Assets resulting from the NADB (FY05) Data Call	Total Number of Assets in the Database
34	New Hampshire	-	-	-	-	-	77
35	New Jersey	610	469	175	37.31%	294	904
36	New Mexico	533	824	9	1.09%	815	1348
37	New York	1634	4187	134	3.20%	4053	5687
38	North Carolina	518	227	25	11.01%	202	720
39	North Dakota	255	537	29	5.40%	508	763
40	Ohio	1135	875	123	14.06%	752	1887
41	Oklahoma	290	35	20	57.14%	15	305
42	Oregon	737	353	250	70.82%	103	840
43	Pennsylvania	617	2298	42	1.83%	2256	2873
44	Rhode Island	70	34	7	20.59%	27	97
45	South Carolina	214	117	23	19.66%	94	308
46	South Dakota	261	129	30	23.26%	99	360
47	Tennessee	763	267	55	20.60%	212	975
48	Texas	988	2960	144	4.86%	2816	3804
49	Utah	174	386	2	0.52%	384	558
50	Vermont	67	10	7	70.00%	3	70
51	Virgin Islands	19	69	2	2.90%	67	86
52	Virginia	1099	3252	120	3.69%	3132	4231
53	Washington	761	2974	85	2.86%	2889	3650
54	West Virginia	240	292	11	3.77%	281	521
55	Wisconsin	517	6667	38	0.57%	6629	7146
56	Wyoming	161	217	9	4.15%	208	369
57	Unlisted	-	-	-	-	-	20
	Totals	**31963**	**48701**	**3846**	**7.90%**	**44855**	**77069**

Appendix G
Major Contributors to this Report

William J. McCarron, Chief Inspector
Carlton Mann, Chief Inspector
Russell Lundberg, Inspector

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Chief of Staff
Deputy Chief of Staff
Assistant Secretary, Policy
Assistant Secretary, Public Affairs
Executive Secretariat
Assistant Secretary for Infrastructure Protection
Assistant Secretary for Grants and Training
DHS OIG Liaison
Audit Liaison, Preparedness
Assistant Secretary, Legislative and Intergovernmental Affairs

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, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov.

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 the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.