Order Code RL33648

CRS Report for Congress

Critical Infrastructure: The National Asset Database

Updated July 16, 2007

John Moteff
Specialist in Science and Technology Policy
Resources, Science, and Industry Division

Prepared for Members and Committees of Congress

Critical Infrastructure: The National Asset Database

Summary

The Office of Infrastructure Protection (OIP) in the Department of Homeland Security (DHS) has been developing and maintaining a National Asset Database. The Database contains information on over 77,000 individual assets, ranging from dams, hazardous materials sites, and nuclear power plants to local festivals, petting zoos, and sporting good stores. The presence of a large number of entries of the latter type (i.e. assets generally perceived as having more local importance than national importance) has attracted much criticism from the press and from Members of Congress. Many critics of the Database have assumed that it is (or should be) DHS's list of the nation's *most* critical assets and are concerned that, in its current form, it is being used inappropriately as the basis upon which federal resources, including infrastructure protection grants, are allocated.

According to DHS, both of those assumptions are wrong. DHS characterizes the National Asset Database not as a list of critical assets, but rather as a national asset inventory providing the 'universe' from which various lists of critical assets are produced. As such, the Department maintains that it represents just the first step in DHS's risk management process outlined in the National Infrastructure Protection Plan. DHS has developed, apparently from the National Asset Database, a list of about 600 assets that it has determined are critical to the nation. Also, while the National Asset Database has been used to support federal grant-making decisions, according to a DHS official, it does not drive those decisions.

In July 2006 the DHS Office of the Inspector General released a report on the National Asset Database. Its primary conclusion was that the Database contained too many unusual and out-of-place assets and recommended that those judged to be of little national significance be removed from the Database. In his written response to the DHS IG report, the Undersecretary of DHS did not concur with this recommendation, asserting that keeping these less than nationally significant assets in the Database gave it a situational awareness that will assist in preparing and responding to a variety of incidents.

Accepting the DHS descriptions of the National Asset Database, questions and issues remain. For example, the National Asset Database seems to have evolved away from its origins as a list of critical infrastructures, perhaps causing the differences in perspective on what the Database is or should be. As an inventory of the nation's assets, the National Asset Database is incomplete, limiting its value in preparing and responding to a wide variety of incidents. Assuring the quality of the information in the Database is important and a never-ending task. If DHS not only keeps the less than nationally significant assets in the Database but adds more of them to make the inventory complete, assuring the quality of the data on these assets may dominate the cost of maintaining the Database, while providing uncertain value. Finally, the information currently contained in the Database carries with it no legal obligations on the owner/operators of the asset. If, however, the Database becomes the basis for regulatory action in the future, what appears in the Database takes on more immediate consequences for both DHS and the owner/operators.

Contents

Introduction 1

A Short Review of the DHS IG Report 1

The National Asset Database: What It Is and What It Is Not 5

What Are Its Intended Uses? 6
- First Step in Identifying Critical Assets and Prioritizing Risk Reduction Activities 7
- Situational Awareness 8
- Basis for Allocating Critical Infrastructure Protection Grants 11

Issues 11
- Quality 12
- What to Keep 13
- A Potential Change in Status for the Database 14
- Congressional Action 14

List of Figures

Figure 1. National Asset Database Entries by Sector 3

Critical Infrastructure: The National Asset Database

Introduction

The Office of Infrastructure Protection (OIP) in the Department of Homeland Security (DHS) has been developing and maintaining a National Asset Database. The Database contains information on a wide range of individual assets, from dams, hazardous materials sites, and nuclear power plants to local festivals, petting zoos, and sporting good stores. The presence of a large number of entries of the latter type (i.e. assets generally perceived as having more local importance than national importance) has attracted much criticism from the press and from Members of Congress. Many critics of the Database have assumed that it is (or should be) DHS's list of the nation's *most* critical assets and are concerned that, in its current form, it is being used inappropriately as the basis upon which federal resources, including infrastructure protection grants, are allocated. According to DHS, both of those assumptions are wrong.

The purpose of this report is to discuss the National Asset Database: what is in it, how it is populated, what the Database apparently is, what it is not, and how it is intended to be used. The report also discusses some of the issues on which Congress could focus its oversight. This report relies primarily on a DHS Office of the Inspector General (DHS IG) report,[1] released on July 11, 2006, but makes reference to other government documents as well.

A Short Review of the DHS IG Report

The genesis of the National Asset Database remains somewhat unclear. A list of critical sites was begun in the spring of 2003 as part of Operation Liberty Shield.[2] The list contained 160 assets, including chemical and hazardous materials sites, nuclear plants, energy facilities, business and finance centers, and more. The assets were selected by the newly formed Protective Services Division within the Office of Infrastructure Protection, in what was then called the Information Analysis and

---

[1] Department of Homeland Security. Office of the Inspector General. *Progress in Developing the National Asset Database.* OIG-06-04. June 2006.

[2] Operation Liberty Shield was a comprehensive national plan to protect the homeland during U.S. operations in Iraq. For a discussion of some of the other initiatives taken as part of Operation Liberty Shield, see CRS Report RS21475, *Operation Liberty Shield: Border, Transportation, and Domestic Security*, by Jennifer E. Lake.

Infrastructure Protection Directorate, Department of Homeland Security. The Secretary of DHS asked states to provide additional security for these sites.[3]

During the course of the year (2003), DHS continued to collect information on various assets from a variety of sources. By early 2004, DHS had accumulated information on 28,368 assets. Although Operation Liberty Shield was now considered over, the initial list of 160 critical assets, those judged to be in need of additional protection because of their vulnerability and the potential consequences if attacked, grew to 1,849 assets and became known as the Protected Measures Target List.[4] It is not clear when the information being gathered became known as the National Asset Database.[5]

By January 2006, according to the DHS IG report, the Database had grown to include 77,069 assets, ranging from nuclear power plants and dams to a casket company and an elevator company. It also contains locations and events ranging from Times Square in New York City to the Mule Day Parade in Columbia Tennessee (which, according to the city's website, draws over 200,000 spectators each year for the week-long event).

The IG report categorized entries in the National Asset Database by critical infrastructure/key resource sector (see **Figure 1**).[6] Additionally, the DHS IG report identified some of the entries with more specificity. For example, the Database contained, at the time, 4,055 malls, shopping centers, and retail outlets; 224 racetracks; 539 theme parks and 163 water parks; 1,305 casinos; 234 retails stores;

---

[3] DHS offered assistance to help protect these sites through its Buffer Zone Protection Plan program. At times the State Homeland Security grants could be used to help pay for overtime of law enforcement officials and National Guardsmen protecting critical sites.

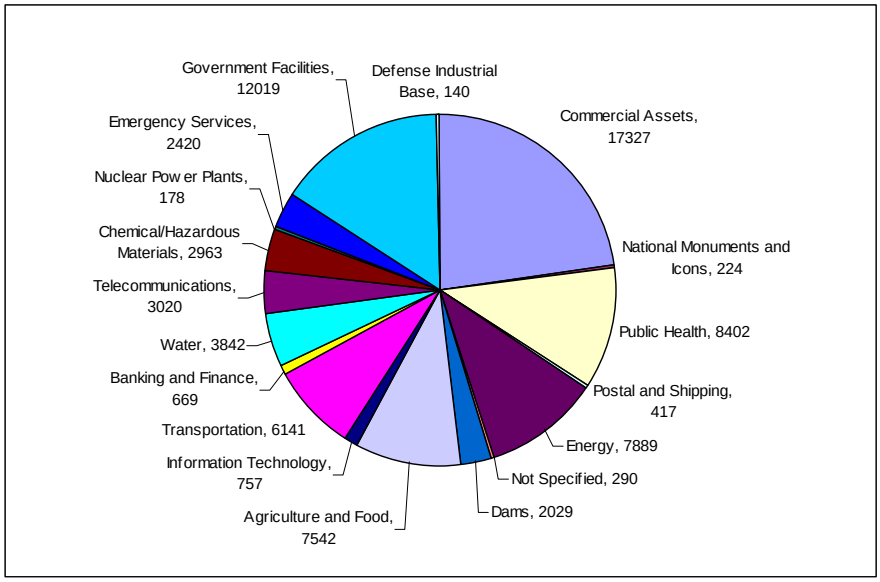
[4] According to testimony by the then Undersecretary for Information Analysis and Infrastructure Protection, a list of 1,700 assets (according to the DHS IG report the actual number was 1,849) was culled from the larger list. However, the DHS IG report implied that the Protected Measures Target List grew independently, to which was added additional information from the states and other sources, leading to a combined list of 28,368 assets, which then grew into the National Asset Database.

[5] In June 2004, the House Appropriations Committee made reference to a Unified National Database of Critical Infrastructure, described as a master database of all existing critical infrastructures in the country. See, U.S. Congress. House of Representatives. *Department of Homeland Security Appropriations Bill, 2005*. H.Rept. 108-541. p. 92. The comparable Senate Appropriations Committee report (S.Rept. 108-280) made reference to a National Asset Database. The budget request for FY2005 mentions the development of a primary database of the nations critical infrastructure, but gave it no name.

[6] The statutory definition of critical infrastructure is given in the USA PATRIOT Act (P.L.107-56). It is: "...systems and assets...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 and safety, or any combination of those matters." There are currently 12 sectors of the economy and 5 groups of key resources (dams, commercial assets, government facilities, national monuments, nuclear facilities) that DHS considers as possessing systems or assets that, if lost, may have a critical impact on the United States.

514 religious meeting places; 127 gas stations; 130 libraries; 4,164 educational facilities; 217 railroad bridges; and 335 petroleum pipelines.

Figure 1. National Asset Database Entries by Sector



Source: Office of the Inspector General. Department of Homeland Security. Taken from *Progress in Developing the National Asset Database.*

The DHS gets information for the Database from a variety of sources. According to the National Infrastructure Protection Plan (NIPP)[7], sources include existing government and commercially available databases;[8] sector-specific agencies and other federal entities; voluntary submittals by owners and operators; periodic requests for information from states and localities and the private sector; and DHS-initiated studies. The number of assets in the Database is expected to grow as additional information is gathered.

The DHS IG report focused much of its attention on information provided by states and localities as the result of two data requests made by DHS. According to the DHS IG report, the vast majority of the 77,069 entries was collected as a result of those requests.

---

[7] Department of Homeland Security. *National Infrastructure Protection Plan*. Released June 30, 2006. See, [http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm].

[8] According to the DHS IG report, examples of existing government databases that have contributed to the National Asset Database include the Chemical Sites List (an Environmental Protection Agency database), and the Government Services Administration list of GSA Buildings.

According to the IG report, the first data call to the states, made by the Office of Domestic Preparedness in 2003, yielded poor quality data.[9] The IG report described the guidance given states and localities as "minimal."[10] The guidance apparently did tell states, however, to "consider any system or asset that, if attacked, would result in catastrophic loss of life and/or catastrophic economic loss."[11] As a result, assets such as the petting zoos, local festivals and other places where people within a community congregate, or local assets ostensibly belonging to one of the critical infrastructure sectors, were among the assets reported. According to the IG report, many state officials were surprised to learn that additional assets from their states were added to the Database, which raises additional questions about how the information was collected.

According to the IG report, the second request to the states for critical infrastructure information came from the Office of Infrastructure Protection in July 2004 and was "significantly more organized and achieved better results."[12] Guidance was more specific, as was the information requested. DHS requested information for 17 data fields. Of those, DHS considered the following to be most important: address, owner, owner type, phone, local law enforcement point of contact, and latitude and longitude coordinates.[13] States were also asked to identify those assets that they felt met a level of national significance. Criteria for identifying assets of national significance was provided by DHS. The criteria described certain thresholds, such as refineries with refining capacity in excess of 225,000 barrels per day, or commercial centers with potential economic loss impact of $10 billion or capacity of more than 35,000 people. Although the request was more specific, states were given much leeway as to what to include, and OIP accepted into the Database every submitted asset.[14] As a result, additional assets of questionable national significance were added to the Database.[15]

The DHS IG report drew two primary conclusions. The first is that the Database contains many "unusual, or out-of-place, assets whose criticality is not readily

---

[9] Department of Homeland Security. Office of the Inspector General. Op. Cit. p. 11. The Office of Domestic Preparedness is now called Grants and Training and is located within the Federal Emergency Management Agency, newly reconstituted by the Post-Katrina Management Reform Act of 2006 (part of the FY2007 DHS appropriation bill). Referred to as ODP throughout this report, it manages the majority of grants to states and localities for homeland security and critical infrastructure protection.

[10] Ibid p. 8.

[11] Ibid p. 8. This is similar language used in ODP's Urban Areas Security Initiative grants.

[12] Ibid. p. 12.

[13] The collection of personal information in the Database requires DHS to publish a Privacy Impact Assessment. That Assessment can be found at [http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nadb.pdf]. A discussion of the Assessment is beyond the scope of this report. Site last visited on July 16, 2007.

[14] Department of Homeland Security. Office of the Inspector General. Op. cit. p. 6.

[15] According to the DHS IG report, the Database contains 11,018 entries identified as nationally significant, 32,631 identified as not considered nationally significant, and 33,419 whose significance are undetermined.

apparent,"[16] while, at the same time, it "may have too few assets in essential areas and may present an incomplete picture."[17] The second conclusion was that the types of assets that were included and the information provided are inconsistent from state to state, locality to locality. For example, California entries included the entire Bay Area Regional Transit System as a single entry, while entries listed for New York City included 739 separate subway stations.[18]

The IG report made 4 recommendations:

- review the National Asset Database for out-of-place assets and assets marked as not nationally significant, and determine whether those assets should remain in the Database;
- provide state homeland security advisers the opportunity to review their assets in the Database to identify previously submitted assets that may not be relevant;
- during future data calls, provide States a list of their respective Database assets to reduce ... duplicate submissions; and
- establish a milestone for the completion of a comprehensive risk assessment of critical infrastructure and key resources and ensure they are accurately captured in the National Infrastructure Protection Plan.

The National Asset Database: What It Is and What It Is Not

The National Strategy for Homeland Security recognized that not all assets within each critical infrastructure sector are equally important, and that the federal government would focus its effort on the highest priorities.[19] The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets stated that DHS will develop a methodology for identifying assets with national-level criticality and using this methodology will build a comprehensive database to catalog these critical assets.[20] Judging from the criticism leveled at it, many believe the National Asset Database is (or should be) DHS's list of assets critical to the nation.

---

[16] Department of Homeland Security. Office of Inspector General. Op. cit. p. 9.

[17] Ibid p. 18.

[18] Other examples of what the DHS IG considered to be inconsistent were: some states listed schools for their sheltering function, some did not; Indiana listed over 8,000 assets, more than states larger in area and population like New York, Texas, and California; and, fewer banking and finance centers are listed for New York than North Dakota.

[19] Office of Homeland Security. *National Strategy for Homeland Security*. July 2002. p. 30.

[20] White House. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. February 2003. p. 23.

However, in his written response to the IG report, the Undersecretary for Preparedness, George Foresman, to whom the Office of Infrastructure Protection reports, stated that the National Asset Database is "not a list of critical assets...[but rather] a national asset inventory...[providing] the 'universe' from which various lists of critical assets are produced."[21] According to the National Infrastructure Protection Plan, the National Asset Database is a comprehensive catalog with descriptive information regarding the assets and systems that comprise the nation's critical infrastructure and key resources.[22] The Assistant Secretary for Infrastructure Protection, Robert Stephan, has called the Database a 'phonebook' of 77,000 facilities, assets and systems from across the nation, needed to facilitate more detailed risk analyses.[23]

Some may ask why there should be this difference in perception regarding the National Asset Database. One possible explanation is that, as noted above, the National Asset Database started out as the Protected Measures Target List, which was a prioritized list of assets considered critical at the national level. Also, as reported in at least one media source, when asked for its list of critical assets, Members of Congress were shown the expanded list containing the questionable assets.[24] Based on subsequent response, Congressional interest appears focused on a prioritized list.

Also, what is meant by the term "critical infrastructure" continues to generate some confusion. The definition provided in the USA PATRIOT Act and in other policy documents refers to specific assets or systems within a selected set of sectors or categories. However, the term also is used often to identify the sectors and categories themselves. For example, the transportation sector is often called a critical infrastructure, when, according to the statutory definition, only those assets within the transportation sector whose loss would be debilitating to the nation should be called critical infrastructure. Given the varied usage of the term critical infrastructure, the National Infrastructure Protection Plan description of the National Asset Database above, is unclear. Is it a list of assets that are critical, or is it a list of assets that make up each of the critical sectors, with criticality to be determined later?

What Are Its Intended Uses?

There appear to be two primary uses for the Database: as a first step in a prioritization process that eventually will help focus risk reduction activities; and, to

---

[21] Department of Homeland Security. Office of Inspector General. Op. cit. p. 29.

[22] Department of Homeland Security. *National Infrastructure Protection Plan*. Op. cit. pg159.

[23] See *USA Today*, "Database is Just the 1st Step," by Robert Stephan. July 21, 2006. p. 8A.

[24] See Congressional Quarterly's internet publication, *CQ Homeland Security*, July 29, 2004, at [http://homeland.cq.com/hs/display.do?docid=1278697&sourcetype=31], last viewed July 16, 2007.

provide a degree of situational awareness. According to Assistant Secretary Stephan, the Database "does not drive the Department's funding decisions."[25]

First Step in Identifying Critical Assets and Prioritizing Risk Reduction Activities

Taking an inventory of one's assets is a standard first step for most risk management processes used to prioritize the protection of those assets.[26] The second step is to screen this initial list for those assets considered critical to the organization (or country) using specific criteria. Further analysis is focused on these critical assets. The National Infrastructure Protection Plan establishes DHS's risk management process. According to the NIPP, identifying the assets that comprise the nation's 17 critical infrastructure sectors and key resources within the National Asset Database represents the first step in its process.

As envisioned by the NIPP, DHS will then select those assets from the Database it considers critical to the nation as a whole.[27] If the asset is judged not to be critical from a national perspective, DHS does not require any further information. If the asset does have the potential to be critical, DHS will ask for more information, which includes information that will support further risk and risk mitigation analysis (e.g. vulnerability to specific forms of attack or natural disasters and more detailed analysis of the consequences associated with the loss of the asset, including interdependencies with other assets). Vulnerability, consequences, and threat information then will be integrated to yield a risk score. According to the NIPP, those assets that pose the greatest risk are further analyzed to identify potential risk reduction initiatives, which are then prioritized (i.e. the risk reduction initiatives) based on their cost-effectiveness. Presumably, as additional analysis and information is generated for a particular asset, it will be added, or linked, to the Database. According to the IG report, DHS officials acknowledge that many of the assets currently in the Database "will never be analyzed in depth or used to support any program activity."[28]

According to the Assistant Secretary, DHS had identified about 600 assets that it considers to be critical to the nation, based on its analysis of vulnerability to attack

---

[25] *USA Today*. Op. cit.

[26] For a discussion on common basic elements of a risk management process, in the context of critical infrastructure protection, see CRS Report RL32561. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threat, Vulnerability, and Consequences*, by John Moteff.

[27] As mentioned above, in the second data request to the states, DHS provided some characteristic thresholds by which DHS may assess whether or not an asset is critical at the national level. Also, according to the NIPP, as the various sectors work with their Sector Specific Agencies to develop sector-level protection plans, another source of information for the Database, owners/operators will have a standard form containing a few questions that can assist in determining criticality.

[28] Department of Homeland Security. Office of Inspector General. Op. cit. p. 10.

or natural events and the possible consequences.[29] This list is apparently prioritized further.[30] The Assistant Secretary asserted that this shorter list does not contain petting zoos, popcorn factories or other such facilities.[31]

While it may be common practice to take an initial inventory of one's assets as a first step in a risk management process, detailed information on individual assets is not necessarily needed to determine their criticality. The presence of gas stations listed in the National Asset Database is a case in point.

Gas stations could be considered a part of the oil and gas infrastructure, a subsector of the energy sector. In assessing the oil and gas infrastructure, one may want to identify, in general, all the assets that make up that infrastructure from production fields, to refineries, to distribution, and all the transport elements in between. Gas stations would be on that list, at the very end of the distribution chain. In determining which assets are the most critical, one does not need specific information on individual gas stations to determine that the loss of any individual gas station would have a minimal effect on the distribution of gasoline throughout the country, or on the economy, or national public health, beyond the immediate vicinity of the gas station itself. Yet the National Asset Database contains 127 gas stations. Unless these 127 specific gas stations have some unique characteristics (perhaps being located next to an identified critical asset which could be damaged if there were a loss of the gas station), maintaining specific information on those gas stations seems unnecessary to determine their criticality.[32]

Situational Awareness

DHS justifies keeping assets that have not been judged as being critical at the national level in the Database as a way to provide a degree of situational awareness.[33]

---

[29] In more recent testimony, before the Senate Committee on Homeland Security and Governmental Affairs, Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration, July 12, 2007, the number of such assets has grown to about 2,500. It is not clear how this list of about 600 assets compares with the earlier Protective Measures Target List. Presumably, the list is a subset of the 77,069 assets in the Database and not a parallel list, but that is not clear either.

[30] See, ABC News Internet Ventures, *Government Confirms Much Shorter List of Critical U.S. Locations,* at [http://www.abcnews.go.com/GMA/print?id=2218846]. Site last viewed July 16, 2007.

[31] *USA Today*. Op. cit.

[32] Gas stations of any size or location are not listed in the criteria of what DHS considers to be a nationally significant asset within the oil and gas sector or any other sector or key resource category.

[33] Neither DHS or the IG report use the term "situational awareness" to describe the activities discussed in this section. This is a term CRS believes captures the breadth of the statements made regarding this particular use of the Database.

Undersecretary Foresman noted in his response to the IG report that, "Many assets not 'critical' are, in fact, critical depending upon the circumstances...."[34] For example, as noted in the NIPP, "...the information may be used to quickly identify those assets...that may be the subject of emergent terrorist statements or interest or that may be located in the areas of greatest impact from natural disasters."[35] According to the NIPP, having this information (apparently regardless of the criticality level of the asset) will help inform decisions made regarding preparedness, response, and recovery to a wide range of incidents and emergencies.[36] In defense of the contents of the National Asset Database, Assistant Secretary Stephan is quoted as saying: "What happens the very first day that al-Qaeda attacks a convenience store chain times a dozen across the country?...we better have some of those things in the database so that we know what that universe of things is that we have to worry about."[37]

According to the FY2007 Congressional Budget Justification for the Infrastructure Protection and Information Security (IP/IS) Program,[38] the Database will deliver something called the Risk/Readiness Dashboard to DHS management. The budget justification identified the Risk/Readiness Dashboard as a planning and management tool that will eventually fuse threat streams with critical infrastructure vulnerability information and consequences, and will visually present a risk profile for critical infrastructure assets. According to the budget justification, such a capability will provide real-time knowledge that can be used to support rapid decision-making during periods of heightened threats.

Also, while a particular asset may not be critical at the national level, it may still be critical at the state or local level. Since DHS plans to allow many stakeholders eventually (with appropriate clearances) to have selected access to the Database, and the information in it or linked to it, the Database represents a common picture (i.e. a standard format and taxonomy) for all to use.[39] Also, according to the

---

[34] Department of Homeland Security. Office of Inspector General. Op. cit. p. 29.

[35] Department of Homeland Security. *National Infrastructure Protection Plan*. Op. cit. p. 32.

[36] It is not clear how, or if, the Database was used to inform preparedness and response decisions made during the hurricanes of 2005.

[37] *The Washington Post*. "U.S. Struggles to Rank Potential Terror Targets. Securing All Sites Not Financially Feasible, but Choices Are Fraught With Uncertainty," by Spencer Hsu. July 16, 2006. p. A9.

[38] The IP/IS program supports much of the Department's critical infrastructure protection activities, including its coordinating responsibilities, the National Infrastructure Protection Plan, the Protected Critical Infrastructure Information Program, etc. It is one of the Preparedness Directorate's Budget Activities.

[39] For example, the FY2007 budget justification discussed a program called Constellation, an automated critical asset management system, which would allow law enforcement to inventory, categorize, prioritize, and database critical assets. It also includes a risk assessment system, compatible with the National Asset Database, and allows for automated BZPP development. Constellation was begun in Los Angeles as a pilot program. The (continued...)

Undersecretary, DHS does not support purging the Database of these non-nationally critical assets, because it is important to the Department to be informed about what is important to the states and localities.[40]

The statements above raise a number of issues. First, that assets may be critical under some circumstances and not others, or become critical because they have been identified by intelligence as possible targets, seems to conflict with the statutory definition of critical infrastructures. Under the conditions stated above, just about any asset could be considered critical and setting and implementing priorities would become even more complicated than it is now. Many would expect DHS to respond to such intelligence as part of its counter-terrorism efforts, which might include quickly deploying critical infrastructure resources such as sending out vulnerability assessment teams and establishing buffer zone protection plans. However, such efforts seem to lie beyond the fundamental goal of the critical infrastructure protection program, which is to identify those assets most critical to the nation as a whole.

Also, if the National Asset Database is meant to be a comprehensive list of the nation's infrastructure assets, regardless of criticality, it is incomplete. As noted in the previous section, only 127 gas stations are in the Database. There are over 167,000 gas stations in the United States.[41] Similarly, the Database contains only 140 defense industrial base assets, 417 postal and shipping sites, 669 banking and financial assets, and 7,542 agriculture and food assets. According to the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, DHS estimated that there are 250,000 defense industrial firms, 137 million postal and shipping delivery sites, 26,600 FDIC insured institutions, and almost 2 million farms and 87,000 food processing plants.[42] To identify only a few a these assets, perhaps in some states, but not in others, limits the utility of the current National Asset Database to support situational awareness to those relatively few instances where the Database may have the appropriate information.

The position that the National Asset Database holds data on those assets that states and localities have identified as important to them is contradicted by the DHS IG report. According to the report, state officials were repeatedly surprised to learn about the assets that were added as part of the ODP data call and which remain in the Database.[43] The Database includes many assets not selected by the states.

---

[39] (...continued)
program is suppose to expand to other cities during FY2007 and information integrated with the National Asset Database.

[40] Department of Homeland Security. Office of Inspector General. Op. cit. p. 31.

[41] *National Petroleum News*. "Market Facts: Mid-July 2006. 2006 NPN Station Count." p. 98.

[42] White House. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Op. Cit. p. 9.

[43] Department of Homeland Security. Office of the Inspector General. Op. cit. p. 12.

Basis for Allocating Critical Infrastructure Protection Grants

The role that the National Asset Database plays in allocating federal resources to states and localities for infrastructure protection is of obvious interest to Congress. In FY2006, allocations of Urban Area Security Initiative grants saw some significant changes based on new risk calculations by the DHS. A number of cities saw their grant levels drop. Some Members believe that allocations were based on what they consider to be a flawed National Asset Database.

Over the last two grant cycles, according to the DHS IG report, ODP has made increased use of information in the National Asset Database to support its allocation of various critical infrastructure protection grants to states and localities. However, according to the Assistant Secretary, the National Asset Database does not drive DHS's funding decisions. The exception is the Buffer Zone Protection Plan grants, which were initiated to support the protection efforts associated with the original Protected Measures Target List and Operation Liberty Shield.

The relationship between the ODP's grant-making process, the National Asset Database, and the NIPP is not explicitly stated in DHS documents. The NIPP risk assessment process was finalized June 30, 2006, but ODP has had some form of risk assessment process in place for determining initial grant allocations for programs such as the Urban Area Security Initiative since 2003. Also, for the FY2006 cycle, ODP indicated it had evaluated over 120,000 specific infrastructure assets,[44] but the National Asset Database only contained 77,069 assets as of January 2006. It would appear that ODP's grant-making process operates independently from both the National Asset Database and the National Infrastructure Protection Plan.[45]

Issues

Assuming that the Undersecretary is not changing the definition of critical infrastructure, and accepting DHS's argument that the National Asset Database is not a prioritized list of critical assets, and that it is not the basis for determining grant allocations, two issues remain: the quality of the information contained in the Database; and, whether the value of keeping low criticality assets in the Database warrant the costs associated with maintaining them in the Database. Another potential issue could arise if the current voluntary nature of the Database changes. Congress may ultimately focus its oversight of the National Asset Database on these areas.

---

[44] See, Department of Homeland Security. Office of Grants and Training. *Discussion of the FY2006 Risk Methodology and the Urban Area Security Initiative* located at [http://www.ojp.usdoj.gov/odp/docs/FY_2006_UASI_Program_Explanation_Paper_011805.doc], last viewed on July 16, 2007.

[45] According to a conversation with Assistant Secretary Stephan, July 12, 2007, the short list of critical assets is forwarded to the Office of Grants and Training (referred to as ODP in this report), to be incorporated into their modeling exercise.

Quality

Data quality is always an issue in generating any database. In the case of the National Asset Database, quality includes accuracy, consistency, and completeness. The quality of the information gathered early in the development of the Database has been questioned. For example, early in the evolution of the list, certain electric utility operators were presented with a list of critical electric power assets drawn up by DHS and noticed that some of the entries were not currently in use.[46] Also, one Member of Congress noted that the location for Disneyland was incorrect.[47] According to the IG report, DHS itself determined that the early Protected Measures Target List was unreliable.[48]

DHS has taken a number of steps to improve the quality of the information contained in the Database. The IG report noted that during the second data call to the states, DHS hired contractors to put the information it received into a consistent format, to research missing information, and to verify the accuracy of the information. DHS has approved a taxonomy which everyone submitting information can use to categorize and subcategorize assets. DHS plans to use this taxonomy in future data calls. The IG report also stated that DHS intends to use expert panels to review information in their sector of expertise. According the FY2007 budget justification, one of the responsibilities of the Protective Security Advisors[49] is to verify critical infrastructure information.

Of particular concern is the completeness of the information included. Beyond the issue that there appears to be an incomplete inventory of the less than critical assets, as noted above, the IG was particularly concerned that the Database does not include assets that one might conclude should be included. The IG attributed part of this problem to reluctance on the part of private sector owner/operators to share certain information with DHS, notwithstanding the Protected Critical Infrastructure Information Program.[50]

Insuring the quality of the information in the Database is likely to require a continuous effort, since quality also implies currency. If a particular site closes, moves, or changes ownership, the changes would logically need to be captured in the Database.

---

[46] Based on personal communication with industry official, September 29, 2003.

[47] Quoted by *CQ Homeland Security*. Op. cit.

[48] Department of Homeland Security. Office of Inspector General. Op. cit. p. 16.

[49] Protective Security Advisors are DHS employees stationed in the field to act as liaison with state and local stakeholders.

[50] The Protected Critical Infrastructure Information Program implements the Critical Infrastructure Information Act of 2002, passed as part of the Homeland Security Act, P.L. 107-296, Title I, Subtitle B. The act provides for a variety of protections of critical infrastructure information submitted voluntarily to the Department, including exemption from the Freedom of Information Act (552 U.S.C. 15). For a discussion of the Critical Infrastructure Information Act see, Archived CRS Report RL31762. *Homeland Security Act of 2002: Critical Infrastructure Information Act.*

The consideration of quality could include also the accessibility, flexibility, and security of the database. The NIPP suggested that the Database would be accessible to many type of queries, by many types of stakeholders. However, it is not clear that the Database yet has these capabilities. DHS intends to develop a second generation Database, one that includes the integration of vulnerability, risk, threat, and other relevant information. According to the IG report, DHS does not expect the second generation Database to be ready for two more years. In regard to security, the Undersecretary, in his response to the IG report, asserted that the Database currently "exceeds all security and protection standards."[51] Assessing the accuracy of this assertion is beyond the scope of this report.

What to Keep

The IG report asserted that maintaining unusual and out-of-place entries in the Database may:

- complicate efforts to develop a useful database;
- make resource allocation more challenging;
- obscure desired data;
- waste time and money in repeatedly filtering them out of analyses or trying to prioritize them; and
- taint credibility.

The DHS IG report, however, does not explain how these entries would necessarily complicate, challenge, and obscure efforts. While the Database may not yet be as accessible or as searchable as eventually planned, it is not clear why less critical (or more critical) data could not be tagged as such. However, the presence of this data does involve cost in time and resources. At the very least, as discussed above, the information collected on all assets must be entered and verified (even the less critical ones) and missing data also may have to be located. Also, additional costs would likely be incurred if any further analysis (such as vulnerability assessment or more detailed consequence analysis) were done on these entries.[52] The budget justification documents do not present data on how much money DHS spends on the Database, or how that expense is broken down. However, Congress did appropriate $20 million for the Database in FY2006.[53]

While the argument could be made that the costs might be marginal, the DHS IG report noted that, currently, those entries identified as not being critical at the

---

[51] Department of Homeland Security. Office of Inspector General. Op. cit. p. 32.

[52] While the NIPP suggests that this would not occur, the NIPP also makes reference to (as do the IG report and the FY2007 budget justification) a "national risk profile." The NIPP describes the national risk profile as a high level summary of the aggregate risk and protective status across all sectors. The IG report makes reference to a contractor developed Gross Consequences of Attack tool that would automatically estimate, across a large number of potential targets held in the Database, the consequences associated with various types of attacks. It is not clear if this includes all entries or just those eventually judged most critical.

[53] U.S. Congress. House of Representatives. *Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2006, and for Other Purposes*. H.Rept. 109-241, accompanying H.R. 2360. p. 71.

national level outnumber, by 3 to 1, those that are identified as critical at the national level. Currently, DHS considers only 600 assets as being the most critical, indicating that less than critical sites could actually dominate the cost of maintaining the Database.

It is not clear how to evaluate the value of maintaining these non-critical assets in the Database, especially if their numbers are under-represented and the risk associated with them is relatively low.

A Potential Change in Status for the Database

Currently the presence of a particular asset in the Database carries with it no specific obligations on the part of the owner/operator. They are not required by statute or regulation to provide information to the Database, per se, or to take any specific actions as a result of having an asset listed.[54] Information solicited by DHS is voluntarily given. Presumably, publicly available information does not require the permission of the owner/operator for it to be included in the Database. However, if ever having an asset on the National Asset Database carries with it some legal or regulatory requirements, then what is in and not in the Database, or adding or removing assets from it, might result in much greater consequences for both the owners/operators and DHS.

Congressional Action

The House of Representatives, as part of the 110th Congress's first 100 hours of legislation, passed H.R. 1, "Implementing the 9/11 Commission Recommendations Act of 2007." Title IX of this act includes a section (Sec. 902) dealing with the National Asset Database. The Section did a number of things. It amended the Homeland Security Act to include the requirement that the Secretary of Homeland Security establish a National Asset Database. It also required the Secretary to establish within this Database a subset of assets that the Secretary determines are most at risk. This subset of assets shall be called the National At-Risk Database. This requirement indicated that the House disagrees with the Undersecretary that the National Asset Database should not include a prioritization of assets.

Section 902 also established a National Asset Database Consortium, made up of representatives from at least two, but no more than four, national laboratories along with officials from other federal agencies with appropriate experience in working with and identifying critical infrastructure. The Consortium is to advise the Secretary on how to identify, generate, organize, and maintain the National Asset Database. In addition, the Secretary is to solicit comments from the Consortium on the appropriateness of the risk methodologies employed by the National Infrastructure Protection Plan and alternative methods for defining risk and identifying specific criteria by which to set priorities. The Secretary is to secure recommendations from the Consortium 60 days after this act is enacted.

---

[54] Note that the Database may contain information associated with regulations which require submission of the information for other regulatory purposes.

The Section also required the Secretary to annually review the Database to examine assets in the Database to determine if the information on these assets is incorrect or if they do not meet national asset guidelines used by the Secretary to determine which assets should remain in the Database. It required the Secretary to remove from the Database any asset whose information is not verifiable or which does not meet the nation asset guidelines. The requirement disagrees with the Undersecretary's position that less-than-nationally-critical assets should remain in the Database.

Also, the Secretary is to provide the Database to states for review and to meet annually with the states to discuss guidelines their submissions of information for the Database. This requirement is in agreement with recommendations made by the Inspector General. Section 902 also required the Secretary to ensure that the information contained in the Database can be organized by sector, state, locality, and region.

Section 902 required the Secretary to report to Congress annually on those assets in the Database considered to be most at risk. The report is to include name, location, and sector of each asset. It is also to include any changes in the criteria used to define or identify critical infrastructure and any changes in the compiling of the Database. It is also to include the extent to which the Database has been used as a tool for allocating resources. It is likely that DHS would classify much of the information specific to particular assets in the Database.

Title XI in the Senate's companion bill, S. 4, "Improving America's Security Act of 2007," also required the Secretary to develop a risk-based prioritized list of critical infrastructure and key resources. The list should consider those assets or systems that, if destroyed or disrupted, by attack or natural catastrophe, would cause significant loss of life, severe economic harm, mass evacuations, or lead to the loss of vital public services. The list should reflect a cross-sector analysis to determine priorities for prevention, protection, recovery, and reconstitution. The act also instructed the Secretary to report to Congress annually the criteria used to create the list, the methodology used to solicit and verify information submitted to the list, and how the list will be used in program activities, including grant making.

No further action on either of these bills has occurred to date.[55]

The House version of the FY2008 Department of Homeland Security Appropriations Bill, H.R. 2638, contained report language directing the National Protection and Programs Directorate to remove from the National Asset Database items it deems insignificant, and encouraged the Directorate to provide states and local partners the opportunity to review their assets listed in the Database and to recommend items for removal. The language also stated that the Directorate should

---

[55] These bills may be combined with other homeland security related legislation. See, Congress Daily PM. "House Will Merge 9/11, Transit Bills And Name Conferees." Monday, July 16, 2007, at [http://nationaljournal.com/pubs/congressdaily/dj070716.htm#6]. Site last visited July 16, 2007.

clarify its guidance when soliciting information to ensure uniform and accurate information. The Senate version (S. 1644) contained no similar language.