Privacy Impact Assessment
for the

National Asset Database (NADB)

January 7, 2006

Contact Point
Sandy Ford Page
Director, Disclosure Office
Department of Homeland Security
Office of the Undersecretary for Information Analysis and Infrastructure Protection
202-282-8522

Reviewing Official
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Purpose

This Privacy Impact Assessment (PIA) examines the privacy implications for the National Asset Database (NADB). The Office of Infrastructure Protection's Protective Security Division (PSD) is responsible for reducing the nation's vulnerability to terrorism by developing and implementing plans to identify and protect critical infrastructure and key assets, and to deny the use of these infrastructures as weapons. To facilitate this responsibility, PSD has built the NADB as a repository of the nation's facilities and assets spanning the 17 Critical Infrastructure and Key Resources (CI & KR).

This PIA covers:

1. What information is being collected and why is this information being collected;
2. The intended use of the agency information;
3. With whom the information will be shared;
4. What notice or opportunities for consent would be provided to individuals regarding information collected;
5. How that information is shared and secured; and
6. Whether a system of records is being created under section 552a of title 5, United States Code (the "Privacy Act").

Background

The Physical Targets Section of PSD has gathered and continues to gather data related to Critical Infrastructure and Key Resources (CI & KR) from a variety of sources in order to compile the NADB. The current data collected has resulted from formal data calls and voluntary submissions from Federal agencies, state and local government, and private sector entities and from review and inclusion of information from Federal and commercial databases regarding CI & KR.

In July 2004, the Office of Infrastructure Protection (DHS/IP) in coordination with the Office of State and Local Coordination, conducted a data call requesting that the 56 States and Territories provide a comprehensive listing of those assets they deemed of national or local importance. This approach has been successful in producing a listing of assets that the 56 States and Territories deem important to their well-being and to that of the United States. DHS-IP made no value judgments on the assets submitted, and included all into the NADB for the purposes of building a "universe" of assets. This inclusive approach provides for an NADB that encompasses all assets, not just those perceived as of high importance.

Section 1 Questions About The Data And Its Purposes

1. What information is to be collected?

The NADB collects basic asset and facility data including, address, physical location, facility point-of-contact (POC) (title, individual, or position) and contact number, security POC (title, individual, or position) and contact number, and asset type data fields relevant to the type of facility. The asset type data fields or attributes of interest, are the detailed facility information used in the risk analysis process.

Additional vulnerability assessment and risk mitigation information may be included for applicable sites. Information may be received from Federal agencies, state and local governments, private entities, open source research (internet) and/or commercial databases. No additional personal information other than name, duty title/position, and business contact information is collected. If additional personal information is required, this PIA will be updated.

The NADB contains descriptions and contact information on infrastructure locations from the 50 states and 6 territories. The NADB includes the following asset sectors:

Agriculture and Food

Banking and Finance

Chemical and Hazardous Materials Industry

Defense Industry Base

Energy

Emergency Services

Information Technology

Telecommunications

Postal and Shipping

Public Health

Transportation

Water

National Monuments and Icons

Commercial Assets

Government Facilities

Dams

Nuclear Power Plants

The asset details will include both common and specific information about the asset.

2. Why is the information being collected?

The Office of Infrastructure Protection's PSD is responsible for reducing the nation's vulnerability to terrorism by developing and implementing plans to identify and protect critical infrastructure and key assets, and to deny the use of these infrastructures as weapons. To facilitate this responsibility, PSD has built the NADB as a repository of the nation's facilities and assets spanning the 17 CI & KR sectors. This information is to be used for infrastructure analysis and threat association. Contact information will be used in order to be able to provide awareness to asset owners/operators if the need arises.

3. Is it relevant and necessary to the purpose for which the system is being designed?

The NADB will directly support Homeland Security operations and activities throughout the United States and its territories by providing, as well as maintaining, infrastructure information and analytical capabilities. In order to be able to carry out these functions, the Office of Infrastructure must have contact information for these assets.

4. What is the intended use of the information?

The intended use of the contact information is to contact the individual should additional information on the facility be required or to provide awareness to the facility in cases of relevant and credible threat reporting. Contact information will additionally be used by DHS to coordinate and facilitate any DHS site assistance visits, vulnerability assessments, or risk mitigation surveys at the specific site. This information will be made available in a phased approach to other federal agencies, state and local homeland security advisors, and then private sector councils or associations. This information will only be made available to those users in the entities who require the data to perform their professional duties, and has the proper clearances for access.

5. What are the sources of the information in the system?

The Physical Targets Section of PSD has gathered and continues to gather data related to CI & KR from a variety of sources in compiling the NADB. Sources of the information include Federal agencies, state and local government organizations, and private sector entities which may include facility owners/operators, Federal and commercial databases and open source research, such as Internet. Sources must provide facility location and POC information in order for asset to be included in the NADB. In cases, where the information was not received directly from the CI & KR, such as databases and open source research, the POC given is contacted in order to verify and validate the information before it is entered into the NADB.

6. Where and how are you acquiring the information?

The current data collected has resulted from formal data calls and voluntary submissions from Federal agencies, state and local government, and private sector entities, and of federal and commercial databases.

7. How will the information be checked for accuracy?

For the initial release of NADB, asset data is validated by IP/PSD and then imported into the NADB and assigned a unique DHS Asset Identifier. Data received is primarily validated and verified for currency and accuracy by DHS-contracted companies. In some cases, data is updated by the source on a quarterly basis. This may involve contacting the facility to verify specific facility information. Initial accuracy will be dependent on the source and refresh rate of the data.

Updates will be submitted from various sources and various means. Inherent in the portal is a verification and validation process to ensure that the information submitted is correct. All information,

regardless of the source, will be verified and validated prior to inclusion in the NADB database. When validating information, the individual contacted is informed of the NADB system processes and of any uses that will be made of the information provided. Any changed asset information will not be updated for viewer use until the changes have been completely verified. This ensures that users do not have access to incorrect information. Once the updates have been verified, users that are approved to see the information based on their role-based access controls will have access to the data.

8. Will the system derive new data or create previously unavailable data about an individual through aggregation for the information collected?

No. Information collected about individuals is tied to the asset. If the individual leaves the position the information will be updated with new contact information.

9. Will the newly derived data be placed on the individual's record?

Not applicable. There is no newly derived data.

10. Can the system make new determinations about an individual that would not be possible without the new data?

No. There is no newly derived data.

11. How will the newly derived data be verified for relevance and accuracy?

Not applicable.

12. Are the data elements described in detail and documented?

Some data elements are described in the NADB schema and data dictionary. Many data fields are currently being determined and defined. Once defined, the asset type data fields will be described in the approved DHS Infrastructure Taxonomy document. No additional personal information other than name, duty title/position, and business contact number is expected to be collected. If additional personal information is required, this PIA will be updated.

Section 2 Questions About Redress

1. What opportunities do individuals have to decline to provide information?

Data submissions are all voluntary. Submissions are provided by Federal agencies, State and Local government organizations, and private sector entities. Information may also be licensed or purchased from commercial databases for inclusion in the NADB.

2. What opportunities do individuals have to consent to particular uses of the information?

Consent is given as a condition to submission.

3. How do individuals grant consent concerning how their information will be used or shared?

Data classified or restricted by the user based on statute or regulations will be followed based on the Original Classification Authority (OCA.) Data will be protected or disseminated based on the classification of the information as classified by the source. Role based access controls are established within the NADB to limit user access to need-to-know and scope of performance.

4. What are the procedures for individuals to gain access to their own information?

Users will have access to facility information based on the user's clearance, need-to-know, and scope of performance. Contact information will be available to those responsible for a particular asset.

5. What are the procedures for correcting erroneous information?

Contractors will conduct verification and validation of asset information. A process flow also exists in the NADB which ensures that changes or added assets are validated, verified, and then approved for inclusion and display in the NADB. See response in question 1.7 above.

Section 3 Questions About Access To The Data

1. Who will have access to the data in the system (users, managers, system administrators, developers and others) and is it documented?

Business case documentation is being finalized. User access will be based on a phased approach in which PSD users will be given access first. The following user communities within IP/PSD will have end user privileges to the NADB:

- Physical Targets Section
- Vulnerability Identification Section
- Protective Measures Section
- Risk Analysis Section
- Field Operations Section

Follow-on users include IAIP, then DHS and other Federal organizations, and state and local homeland security offices. Future release of the NADB end users are projected to expand to include:

- Information Analysis and Infrastructure Protection (IAIP) Directorate
- Other DHS Directorates
- Federal Government Agencies
- State Governments
- Territorial Governments

- Local Governments
- Tribal Governments
- Private Sector

Timeline for release will be outlined in the NADB Operations documents.

2. How will access to the data by a user be determined?

Inherent in the NADB is the ability to apply for user access. Role based access controls in place to ensure user access is based on need-to-know, scope of performance, and clearance level. User access requests will be verified to ensure scope of performance, and clearances will be verified in coordination with the DHS Security Office. Individual role-based access controls for each user will be determined by the NADB Program Manager (PSD).

3. Are criteria, procedures, controls, and responsibilities regarding access documented?

Role Based Access Controls: All users will have to apply and be approved for access to the NADB. Access to the NADB will be given to only those users with both the need-to-know and the required clearances(s). The approval process will verify prospective user's security clearance and scope of use. User's access will be limited to specific applications and data based on his/her need-to-know, clearance level and position/scope of authority. The role-based access controls will be outlined in the NADB Business Case and detailed in the NADB Standard Operating Procedures.

4. Will users have role-based access to data on the system limiting them to some but not all of the data?

Yes, the system is role-based and users will only have access to data determined by their roles. The role(s) given to a user dictates what he/she can see and do within the application. This prevents a user from seeing features or data that they do not have rights to view. For example, the data entry and edit features will not be visible to users who do not have rights to add or modify data. Certain users will merely have read-only access to the data while others may be able to download information into a writeable format. Access can also be limited to specific data elements categorized by classification, sector or locality. As an example, State representatives will have access only to their State, and Sector Specific Agencies will only have access to assets in their sector. Some individual users will require multiple sectors or states to facilitate analysis of the State/Sector interdependencies. This feature limits a user' access to specific applications and data, and gives the administrators more control of the system and protection of the data.

5. What controls are in place to prevent the misuse of data by those having access?

Network Security Restrictions: The NADB-SECRET is the first operational production system and will be accessible only to those with access to the SIPRNET (SECRET LAN). Future unclassified and classified production systems will be integrated with the HSIN/HSDN LANs. These networks have implemented security precautions inherent to the LANs. All users are required to sign non-disclosure agreements prior to access to the system.

6. Do other systems share data or have access to data in this system?

The NADB will be a web-based portal integrated with numerous other commercial and Federal databases, geospatial viewers (ICAV, iMAP), vulnerability libraries, threat reporting (NTIDB), among others. Each system will be owned, operated and maintained by the respective originating organization. Data will be restricted and protected by the respective owners. In order to gain access to the NADB data, user access must be requested. Access and the assigned user access roles will be dependant on user clearance, need-to-know, and scope of performance. Users will have access only to that information which is within their professional responsibility.

Users will be notified of the fact that Point of Contact information may be shared and under what circumstances in the Privacy Act notice on the web site.

7. Will other agencies share data or have access to data in this system?

Yes. Asset information, which may include contact name, title, and number, may be exchanged with other agencies. In order to gain access to the NADB data, other agencies must request access. Access and the assigned user access roles will be dependant on user clearance, need-to-know, and scope of performance. Users will have access only to that information which is within their professional responsibility.

8. How will the data be used by these other agencies?

Information in the NADB will be provided to only those entities who are involved in the identification and protection of national infrastructure. NADB information will allow users to identify and understand threats, assess vulnerabilities, and determine potential impacts. Contact information will provide the ability to disseminate timely information to our homeland security partners and the asset owners/operators.

9. Who is responsible for assuring proper use of the data by other agencies?

DHS realizes that the information included in the NADB can be considered sensitive and accepts the requirement for possible dissemination restrictions as per current law, statute regulation. DHS is taking every feasible measure to protect the information and ensure that the data and license restrictions are enforced. The protection of the NADB focuses on both system integrity and security, as well as protection of the data therein. All system integrations with non-DHS entities will require Memorandum of Understandings (MOU) and/or Interagency Security Agreements (ISAs). Individual users will be required to sign non-disclosure agreements prior to receiving access to the data.

10. How will the system ensure that other agencies only get the information they are entitled to?

The application utilizes single sign-on to access the data. This allows the user to login once through an encrypted connection to access multiple applications. Strict requirements have been implemented to enforce a high level of security when logging. The user's password must meet complexity

requirements and after three unsuccessful login attempts the user's account is locked out until an administrator unlocks it. These features help to create secure login environment.

Role-based access controls are implemented to ensure users only have access to the information within their scope of performance. (See 3.4)

Section 4 Questions About Maintenance And Administrative Controls

1. How will the information be secured and is it consistent with agency requirements under the Federal Information Security Act? Specifically:

a. Affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured;

The facility implements approved security protocols and risk mitigation measures required to house such information and system architecture. The facility and system architecture has been accredited for use by the DHS Chief of Information Operations (CIO) office.

Hardware Architecture: The system configuration is designed for a highly available, highly scalable, and highly secure architecture utilizing Oracle Real Application Clusters (RAC) technology. The system is designed to easily handle 1,000 concurrent users, has multiple layers of redundancy for maximum availability, and is able to easily add additional servers as the system requirements grow. The RAC configuration also employs a dual firewall system for added security, ensuring there is only one point of access to the data and that no direct access to the database server from the Internet is permitted. The dual firewalls consist of a perimeter firewall between the Internet and the portal that limits the available ports' incoming connections that are allowed to gain access to the system, and a second interior firewall that limits database access so that it may only receive incoming requests from the Application Server mid-tier servers. This ensures access allowance through the firewalls to the NADB portal only to approved users.

b. Acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls;

Software Security Functions

Beyond the physical security restrictions and the network security restrictions, the NADB application has multiple security mechanisms that have been implemented to provide additional security features. Utilization of login restrictions, session tracking and monitoring, data labeling/tagging of classified information, role based access controls, and advanced auditing ensure proper security of the application.

The DHS CIO has additionally accredited the system and approved the NADB for an interim authority to operate. Final accreditation to allow for a fully operational system has been completed and we

are currently awaiting the final approval/report. This accreditation ensures that the system meets the security and architecture requirements dictated by DHS.

c. Describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information.

Advanced Auditing: Through the audit capability an administrator can see any actions a user has performed and undo any malicious behavior as necessary. This feature enforces accountability for a user's actions within the application. Similarly, any submissions to update or add asset information will be validated and verified prior to approval for inclusion in the NADB for applicable users to access.

Operational Testing and Evaluation(OT&E): OT&E of system functionalities and capabilities are conducted semi-annually, or more often as software upgrades are provided. OT&E includes the assessment of information protection, safeguards, and correct functionalities for the role-based access controls.

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The system will initially be located at a single facility as a web-based portal. Multiple sites are expected in the future. Data between the sites will be integrated into a single hub to ensure consistent and common data fields among the numerous sites.

3. What are the retention periods of data in the system?

Data will be maintained in the NADB as long as the NADB is operational. Refresh rates and verification of accuracy will be dependent on the source of the data, quantity of data, and means of verification.

IAIP is working with the National Archives and Records Administration (NARA) to obtain approval of a records retention and disposal schedule to cover records in this database.

4. What are the procedures for expunging the data at the end of the retention period and are these procedures documented?

In the absence of an approved retention and disposal schedule, DHS lacks the authority to define a retention period or destroy Federal records. Accordingly, until an approved records retention and disposal schedule is established, NADB records will be retained indefinitely.

5. Will the system provide the capability to monitor individuals or groups of individuals?

No.

6. What controls are in place to prevent unauthorized monitoring of individuals or groups of individuals?

The NADB does not have any capabilities to monitor or trace individuals.

7. Under which Systems of Record Notice (SORN) does the system operate?

The collection of contact information is covered by the DHS System of Records Notice 002 published December 6, 2004 69 Fed Reg 70460 DHS/ALL 002.

Section 5 Decision Analysis

1. Did you evaluate competing technologies on their privacy handling capabilities?

No, systems were evaluated on data handling capabilities. All ORACLE and LINUS based solutions contain similar protections.

2. Were any choice changes made to system architectures, hardware, software, or implementation plans as a result of doing a PIA?

No, system hardware and software in place meet all requirements for system and data protection. The system is designed to use as little personal information as possible to meet the needs of the Department in being able to contact individuals responsible for CI & KR.

Responsible Officials

Sandy Ford Page, Director

Disclosure Office, Department of Homeland Security

Office of the Undersecretary for Information Analysis and Infrastructure Protection

202-282-8522

Approval Signature

_____ January 7, 2006

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security