

Appendix 3C: National Asset Database

3C.1 Why Do We Need a National CI/KR Inventory?

HSPD-7 directs the Secretary of Homeland Security to lead efforts to reduce the Nation's vulnerability to terrorism and deny the use of infrastructure as a weapon by developing, coordinating, integrating, and implementing plans and programs that identify, catalog, prioritize, and protect CI/KR in cooperation with all levels of government and private sector entities. A central Federal data repository for analysis and integration is required to provide DHS with the capability to identify, collect, catalog, and maintain a national inventory of information on assets, systems, networks, and functions that may be critical to the Nation's well being, economy, and security. This inventory is also essential to help inform decisionmaking and specific response and recovery activities pertaining to natural disasters and other emergencies.

To fulfill this need, DHS has developed the NADB, a continually evolving and comprehensive catalog of the assets, systems, and networks that comprise the Nation's CI/KR. The NADB contains descriptive information regarding CI/KR and is the primary Federal repository for CI/KR information. Although the NADB is not a listing of prioritized assets, it has the capability to be queried in many ways that can help inform risk-mitigation activities across the CI/KR sectors and government jurisdictions.

3C.2 How Does the Inventory Support the NIPP?

The NADB provides a coordinated and consistent framework to incorporate and display the CI/KR data submitted by Federal, State, and local agencies; the private sector; and integrated Federal or commercial databases. The framework and structure of the NADB have been constructed to readily integrate and provide the required data in a usable and effective manner. Two primary components of this framework are the categorization structure and the infrastructure type data fields:

- The **categorization structure** groups CI/KR by sector and identifies overlaps between and across sectors. It was developed in coordination with the SSAs to ensure that every CI/KR type is represented.

- The **infrastructure type data fields** outline the attributes of interest that are integral to assessment and analysis per a specific category of CI/KR. The information contained in these data fields feeds the strategic risk assessment process used to prioritize CI/KR in the context of terrorist threats or incidents, natural disasters, or other emergencies.

The information in the NADB enables the analysis necessary to determine which assets, systems, and networks comprise the Nation’s CI/KR, and to inform security planning and preparedness, resource investments, and post-incident response and recovery activities within and across sectors and governmental jurisdictions.

3C.3 What Is the Current Content of the Inventory?

- DHS gathers data related to the Nation’s CI/KR from a variety of sources. The present inventory reflects a collection of information garnered from formal data calls, voluntary additions, and the leveraging of various Federal and commercial databases. Information for the database is received from Federal agencies, State and local submissions, voluntary private sector submissions, commercial demographics products, external data sources, and subject matter experts. The information is used to inform CI/KR protection efforts, contingency planning, planning for implementation of initiatives such as the BZPP, and to aid decisionmakers during response, recovery, and restoration following terrorist attacks, natural disasters, or other emergencies.

3C.4 How Will the Current Inventory Remain Accurate?

DHS continues to seek input from multiple sources, including existing databases managed by SSAs, commercial providers, State and local governments, and the private sector. Integrating existing databases will provide a dynamic common operating interface of infrastructure and vulnerability information through a cross flow of data between separate databases, or links to provide access to other databases. Existing databases being considered for integration are shown in table 3C-1. Ownership and control of the data will be determined according to the circumstances of each database. Classification of the data will be based on Original Classification Authority (OCA) guidance and will be protected as required by OCA guidance and direction.

Table 3C-1: Database Integration

Database	Use
Infrastructure and Critical Asset Viewer (iCAV)	DHS is leveraging existing geospatial capabilities and technology used by the National Geospatial-Intelligence Agency by implementing the iCAV as a DHS Geospatial Enterprise Solution for geospatial mapping, analysis, and sorting of the Nation’s CI/KR. The iCAV system will use the geospatial component to spatially display and map information contained in the NADB.
National Threat Incident Database	This database provides a source of consolidated information concerning credible threats and incidents related to our Nation’s CI/KR.
DHS LENS Vulnerability Databases	These databases contain Common Vulnerability and Potential Terrorist Activity Indicator Reports, and site assistance visits and BZPP schedules. Site assistance visits and BZPP documents will be available through classified and unclassified secure portals as applicable.
Commercial/Sector-Specific Databases	Many existing Federal and commercial databases contain information sets pertinent to the NADB. Commercial databases will be purchased based on available funding and priorities for information requirements. An example of one such commercially available database is iMapData, a Web-based geospatial subscription service with access to geo-referenced data sets covering physical infrastructure, emergency services, government facilities, political boundaries, military installations, media distribution areas, educational facilities, business locations, and demographic breakdowns.

3C.5 How Will the Database Be Maintained?

The process of ensuring that the data collected is both current and accurate, and that user requirements are incorporated into the portal as necessary, is continual. Data updates and currency are largely dependent upon the sources of the data and the frequency of the updates that they provide.

Efficiency and reliability have been maintained through the implementation of unique numerical identifiers designed to facilitate the efficient integration of information from multiple databases. Verification and validation efforts by contracted companies or Federal employees will play a key role in ensuring information currency. Eventually, all approved users given access to the NADB will have the ability to provide updated information to the NADB Program Office for review prior to inclusion in the inventory.

Feedback forms are also incorporated to provide user recommendations, changes, requirements, and/or feedback to DHS. User requirements will help drive capabilities and functionality of future evolutions and versions of the inventory.

3C.6 What Are the Security Partner Roles and Responsibilities?

The development and population of the NADB is highly dependent upon the participation and support of the SSAs, the States, and private sector entities:

- SSAs have primary responsibility for providing sector information to DHS for inclusion in the NADB using the format and categorization system employed by the NADB.³⁷ The processes used for sector CI/KR and database identification in coordination with security partners will be described in the SSPs.
- Some State governments have either already developed infrastructure databases or have begun the process to identify and assess CI/KR within their jurisdictions. State homeland security advisors should work closely with DHS and the SSAs to ensure that data collection efforts are streamlined, coordinated, and reflect the most accurate data possible.
- The most current and accurate data are best known by CI/KR owners and operators themselves. Thus, as the owners and operators of the majority of the Nation's CI/KR, private sector entities are encouraged to be actively involved in the development and population of the NADB. Primarily through the voluntary provision of CI/KR information and industry-specific subject matter expertise, the private sector is playing an integral role in the expansion of the NADB.

3C.7 What Are the Plans for NADB Expansion?

The current NADB incorporates a flexible design to facilitate evolution, growth, and continued interconnectivity with additional databases and tools. Advancements will include integration with multiple commercial and Federal CI/KR databases, vulnerability assessment tools and libraries, intelligence and threat reporting databases, and geospatial tools into a single, integrated, Web-based portal.

DHS is developing the next-generation NADB with a more versatile platform to better support integration of DHS and SSA mission-specific applications and mission-specific databases. The goal of this effort is to create a national CI/KR inventory that more efficiently and effectively supports the implementation of NIPP risk management framework activities, including:

- Integration of vulnerability, consequence, and asset/system/network attribute data into a single portal interface to be used as the foundation for the NIPP risk assessment process;
- Access to threat data to support the development of asset, system, and network risk scores;

³⁷ The DHS/OIP taxonomy is the foundation for multiple DHS programs that focus on CI/KR, such as the NADB and the National Threat Incident Database, and should provide the foundation for the lexicon used in the SSPs. This common framework will allow more efficient integration and transfer of information, as well as a more effective analytical tool for making comparisons.

- Assessment and, if appropriate, prioritization of assets, systems, and networks across sectors and jurisdictions based on risk to promote the more effective allocation and use of available resources and to inform planning, threat response, and post-incident restoration actions at all levels of government and the private sector;
- Sharing of consistent information so that all partners involved in CI/KR protection operate from a common frame of reference;
- Acting as a primary information and integration hub for protective security needs throughout the country in support of DHS- and SSA-led activities;
- Supporting the efforts of law enforcement agencies during National Security Special Events and other high-priority security events; and
- Supporting the efforts of primary Federal agencies in responding to and recovering from major natural or manmade disasters.