REQUEST FOR RECORDS DISPOSITION AUTHORITY	LEAVE BLANK (NARA use only) JOB NUMBER N1-563-08-14
To: NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD, COLLEGE PARK, MID 20740-6001	Date Received 1-24-2008
1. FROM (Agency or establishment) **Department of Homeland Security**	NOTIFICATION TO AGENCY
2. MAJOR SUB DIVISION **National Protection Programs Directorate**	In accordance with the provisions of 44 U.S.C 3303a, the disposition request, including amendments is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.
3. MINOR SUBDIVISION **Office of Infrastructure Protection**	
4. NAME OF PERSON WITH WHOM TO CONFER **Kathy Schultz** / 5. TELEPHONE **202-447-5075**	DATE 8-28-08 / ARCHIVIST OF THE UNITED STATES Adrienne C. Thomas

6. **AGENCY CERTIFICATION**

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal on the attached **2** page(s) are not needed now for the business of this agency or will not be needed after the retention periods specified; and that written concurrence from the General Accounting Office, under the provisions of Title 8 the GAO Manual for Guidance of Federal Agencies,

☒ is not required ☐ is attached; or ☐ has been requested.

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
1/16/08	Kathleen A. Schultz	**Senior Records Officer**

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
1	**See attached sheet(s) for:** **Infrastructure Information Collection Program (IICP)** **Inputs, Outputs and System Documentation are covered by GRS 20** User information covered by GRS 24/6a.		

NW 9/2/08 copies sent to Agency, NWMW, NR

National Protection and Programs Directorate

Infrastructure Information Collection Program (IICP)

NARA #

Homeland Security Presidential Directive 7 (HSPD-7) (Critical Infrastructure Identification, Prioritization, and Protection) is a national policy for federal departments and agencies to identify and prioritize the United States' Critical Infrastructure and Key Resources (CI & KR). The Office of Infrastructure Protection Infrastructure Information Collection Division (IICD) is responsible for reducing the nation's vulnerability to terrorism by developing and implementing plans to identify and protect critical infrastructure and key resources, and to deny the use of these infrastructures as weapons.

On June 15, 2006, DHS published the National Infrastructure Protection Plan (NIPP) to clearly define critical infrastructure protection roles and responsibilities. Key to both documents is the need for a central database of risk-related infrastructure attributes to inform risk identification and analysis, and the protection of significant infrastructure. The Infrastructure Information Collection Program (IICP) supports the requirements for collecting, cataloguing, and maintaining standardized and quantifiable infrastructure information to enable the execution of national risk management for CI/KR and for prioritizing the data for use by homeland security partners.

Other authorities or guidance that provides strategic guidance for the IICP include:
- P.L. 107-296: The Homeland Security Act of 2002;
- P.L. 108-458: The Intelligence Reform and Terrorism Prevention Act of 2004;
- National Strategy for Homeland Security, July 2002;
- Executive Order 12472, Assignment of National Security and Emergency Preparedness Responsibilities, April 1984;
- The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, February 2003;
- The National Response Plan;
- The National Preparedness Goal; and
- Office of Infrastructure Protection, Risk Management Division Strategic Goals.

The IICP is expected to consolidate and leverage at least four existing Office of Infrastructure Protection (OIP) programs that directly contribute to the functions of the IICP, and will eliminate any redundancy between these programs. The four programs are:
- Automated Critical Asset Management System (ACAMS): ACAMS is a Web based tool that enables the collection of risk specific infrastructure information from owners/operators, law enforcement and first responders.
- National Asset Database (NADB): The NADB is a virtual repository of CI/KR data.
- Methodology Technical Implementation (MTI): The MTI program develops methodologies and standards for complex infrastructure through the use of scalable common metrics which enables cross-sector risk comparisons.
- Vulnerability Identification Self Assessment Tool (ViSAT): The ViSAT program develops methodologies and standards for non-complex infrastructure through the use of scalable common metrics which enables cross-sector risk comparisons.

The IICP is a web-based portal integrated with numerous other commercial and Federal databases, geospatial viewers (ICAV, iMAP), vulnerability

libraries, threat reporting tools, among others. 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.

Master File / Data:

Asset and Facility Data

The IICP will collect basic asset and facility data to include 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 (attributes of interest) are the detailed facility information used in the risk analysis process. Additional vulnerability assessment and risk mitigation information will be included for applicable sites. Files are queried and sorted based on the analysis required.

The information is required to meet DHS infrastructure protection and homeland security mission roles. Data will be maintained in the IICP as long as the there is an operational requirement. Refresh rates and data verification will be dependent on the information requirements, the source of the data, quantity of data, and available means of verification.

Disposition:

TEMPORARY. Cut off on date of verification of account inactivity or modification. Delete 3 years from cutoff, or until no longer needed for business purposes, whichever is later.