REQUEST FOR RECORDS DISPOSITION AUTHORITY

LEAVE BLANK (NARA use only)

JOB NUMBER N1-563-08-31

To: NATIONAL ARCHIVES & RECORDS ADMINISTRATION
8601 ADELPHI ROAD, COLLEGE PARK, MID 20740-6001

Date Received 7/7/08

1. FROM (Agency or establishment)
Department of Homeland Security

2. MAJOR SUB DIVISION
National Protection and Programs Directorate

3. MINOR SUBDIVISION
Office of Infrastructure Protection

NOTIFICATION TO AGENCY

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request, including amendments is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.

4. NAME OF PERSON WITH WHOM TO CONFER	5. TELEPHONE	DATE	ARCHIVIST OF THE UNITED STATES
Kathy Schultz	**202-447-5075**	6/22/09	Adrienne 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 3 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
7/1/08	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 GRS OR SUPERSEDED JOB CITATION	10.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:** **NPPD/Office of Infrastructure Protection (IP) Program Records**		

N1-563-08-31

U.S. Department of Homeland Security
Headquarters Records Schedules

National Protection and Programs Directorate

The mission of the Office of Infrastructure Protection (OIP) is based on the requirements of the Homeland Security Act of 2002, The Intelligence Reform and Terrorism Prevention Act of 2004, Homeland Security Presidential Directive (HSPD)-7, "Critical Infrastructure Identification, Prioritization, and Protection," Section 550 of the Fiscal Year 2007 Homeland Security Appropriations Act, HSPD-19, "Combating Terrorist Use of Explosives in the United States," and additional Executive Orders, HSPDs and National Security Presidential Directives.

The Office of Infrastructure Protection leads the coordinated national effort to reduce risk to our critical infrastructures and key resources (CIKR) posed by acts of terrorism and enables national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

• Chemical Security Compliance Division (CSCD). CSCD leads the implementation of the Chemical Facility Anti-Terrorism Standards (CFATS), balancing regulatory authority with the need to secure the nation's highest risk chemical facilities while sustaining the economic vitality of the chemical sector. It develops and implements a program that aggressively assesses high-risk chemical facilities, promotes collaborative security planning, and ensures that covered facilities meet risk-based performance standards.

• Infrastructure Information Collection Division (IICD). IICD leads the Department's efforts to acquire and provide standardized, relevant, and customer focused infrastructure data to various public and private sector homeland security partners.

• Infrastructure Analysis and Strategy Division (IASD). IASD leads the nation's premiere analytical teams in the conduct of critical infrastructure and key sources (CIKR)-related modeling, simulation, and analysis in close collaboration with the Department and National Infrastructure Protection Plan (NIPP) partners.

• Protective Security Coordination Division (PSCD). PSCD reduces the risk of the nation's critical infrastructures and key resources of a terrorist attack by assessing vulnerabilities and consequences, and developing, implementing and providing national coordination for protective programs and facilitating CIKR response and recovery operations in an all-hazards environment.

• Contingency Planning and Incident Management Division (CPIMD). CPIMD coordinates and implements the Office of Infrastructure Protection's critical infrastructures and key resources preparedness activities in the areas of exercises, contingency planning, concepts of operations development, and incident management in a manner that is consistent with and supportive of the NIPP and the National Response Framework (NRF), as well as established Department and federal interagency incident management coordination structures.

• Partnership and Outreach Division (POD). POD develops and sustains viable strategic relationships and information sharing systems and processes with the owners and operators of the nation's critical infrastructures and key resources that support program execution across the spectrum of preparedness, prevention, protection, response, and recovery activities. Additionally, POD provides coordination tracks progress of NIPP and SSP implementation, including performance metrics.

• Sector Specific Agency Mission. In addition to these missions, OIP serves as the Site Specific Agency (SSA) for five of the 17 CIKR Sectors — Chemical, Commercial Facilities, Dams, Emergency Services, and Nuclear. OIP is responsible for providing guidance to and coordinating the implementation of the NIPP framework for these five sectors, as well as ensuring that CIKR protection activities are fully integrated across all 17 sectors.

Unless otherwise noted, all disposition instructions are media neutral; they apply regardless of the media or format of the records.

1 Incident Reports

Includes, but is not limited to, finished analysis and associated background material for published documents describing threats/risks to Critical Infrastructure/Key Resources (CI/KR). Information may be used in conjunction with agency Intelligence Case Files. Final reporting distributed to support DHS Components, Federal, State and Local Governments.

a. Pre-Event Reports
These are records of modeling, simulations, and analyses to address critical infrastructure and key resources (CI/KR) protection and preparedness issues related to natural and manmade disasters.

Disposition: PERMANENT. Cut off at end of calendar year in which analysis is complete. Transfer to the National Archives 20 years after cutoff.

NOTE: This transfer instruction applies only to the paper or hardcopy version of these records. When/if DHS decides to transfer these records to the National Archives in an electronic format, DHS and the National Archives will develop appropriate transfer instructions at that time to cover the electronic records.

Additional Information:
Date Span: 2004-present
Year of First Transfer to NARA: 2009
Estimated Current Volume: less than 1 cubic foot
Estimated Annual Accumulation: Unknown

b. Incident Reports: Related to Catastrophic Events
These records consist of reports made during or after an incident related to domestic catastrophic events such as, Hurricane's Hugo and Katrina.

Disposition: PERMANENT. Cut off at end of calendar year of incident. Transfer to the National Archives 20 years after cutoff.

NOTE: This transfer instruction applies only to the paper or hardcopy version of these records. When/if DHS decides to transfer these records to the National Archives in an electronic format, DHS and the National Archives will develop appropriate transfer instructions at that time to cover the electronic records.

Additional Information:
Date Span: 2004-present
Year of First Transfer to NARA: 2009
Estimated Current Volume: less than 1 cubic foot
Estimated Annual Accumulation: Unknown

c. Incident Reports: All Others
These are records of minor incidents not related to significant events.

Disposition: TEMPORARY. Cut off at end of calendar year of incident. Destroy or delete 10 years after cutoff.

2 National Infrastructure Protection Plan (NIPP)/ Sector-Specific Plans (SSPs)

The National Infrastructure Protection Plan (NIPP) and supporting Sector-Specific Plans (SSPs) provide a coordinated approach to critical infrastructure and key resources (CIKR) protection and outlines roles and responsibilities for federal, state, local, tribal, and private sector CIKR partners. The NIPP sets national priorities, goals, and requirements for effective distribution of funding and resources which will help ensure that our government, economy, and public services continue in the event of a terrorist attack or other disaster.

Each Sector-Specific Agency is responsible for developing and implementing a Sector-Specific Plan (SSP), which details the application of the NIPP framework to the unique characteristics and conditions of their sector.

Disposition: PERMANENT. Cut off at end of calendar year in which report is published. Transfer to the National Archives 5 years after cutoff.

Additional Information:
Date Span: 2004-present
Year of First Transfer to NARA: 2009
Estimated Current Volume: 1 cubic foot
Estimated Annual Accumulation: Unknown

3 National Infrastructure Protection Program Files

Records documenting opinions, analysis, or interpretations submitted in support of the NIPP. May include, but are not limited to, documentation of interpretive rulings, program-specific background materials and memoranda, records of concurrence, comments, clearances, justifications, and other issuance records.

Disposition: TEMPORARY. Cut off at end of calendar year when current plan is superseded or obsolete. Destroy or delete 6 years after cutoff.

4 Special Events and Exercises Files

Contains internal memoranda, reports, photographs, maps and other planning documentation accumulated by all action offices in connection with both routine and special events, National Special Security Events (NSSE), and exercises such as Jamestown 2007 Commemoration, TOPOFF 4 (IL for Guam, AZ, and OR), United Nations General Assembly, Major League Baseball's All-Star Game, 2006 and 2007 State of the Union Address and similar protective or special events.

a. Records documenting National Special Security Events (NSSE)

Disposition: TEMPORARY. Cut off at end of calendar year in which event occurred. Destroy or delete 25 years after cutoff.

b. Records reflecting all other events/exercises

Disposition: TEMPORARY. Cut off at end of calendar year in which event or exercise occurred. Destroy or delete 10 years after cutoff.

N1-563-08-31

5 Technology Transition Agreements (TTA)

An agreement between DHS components and related CIKR Sector Specific Agencies to identify critical technological gaps and needs within CIKR; it documents the fiscal and transition commitment of participants in the transition stream to develop, deliver, and integrate a technology/product. TTA defines the functional responsibilities and support relationships between the parties signing the agreement and ensures a clear understanding of the responsibilities of all parties. TTA'S are not legally binding, and parties to the agreement may modify its contents with the concurrence of all parties.

Disposition: TEMPORARY. Cut off at end of calendar year when agreement is terminated. Destroy or delete 3 years after cutoff.

Superseded by:
DAA-0563-2013-0006-0001
DATE (MM/DD/YYYY):
12/02/2014

6 Vulnerability Assessment Files

Files maintained for each assessment may include, but are not limited to, copies of authorizations; preparation instructions; correspondence, memoranda, survey forms, risk assessments, and reports created and collected during the course of surveys and studies on critical infrastructures and key resources

a. Project file (excluding Final Report)
May include, but is not limited to, correspondence on vulnerability assessments, working files, drafts, standards, studies, and work plans.

Disposition: TEMPORARY. Cut off at end of calendar year in which the assessment is completed or cancelled. Destroy or delete 25 years after cutoff or 3 years after responsible office determines it is no longer needed for legal, audit, administrative or business purposes.

b. Final Report

1) Tier 1 and Tier 2 CIKR Assessments and National Special Security Events (NSSE)
These records cover CIKR that were designated Tier 1 or Tier 2 at the time of the assessment.

Disposition: TEMPORARY. Cut off at end of calendar year in which the assessment is completed. Destroy or delete 99 years after cutoff.

2) All Other Assessments

Disposition: TEMPORARY. Cut off at end of calendar year in which the assessment is completed. Destroy or delete 25 years after cutoff.

c. Projects not implemented

Disposition: TEMPORARY. Cut off on date of decision to decline. Destroy or delete 5 years after cutoff or when no longer needed for business purposes, whichever is later.