REQUEST FOR RECORDS DISPOSITION AUTHORITY

LEAVE BLANK (NARA use only)

JOB NUMBER N1-563-04-9

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

Date Received 2-10-2004

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

2 MAJOR SUB DIVISION
Information Analysis and Infrastructure Protection

3. MINOR SUBDIVISION
Critical 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request, including amendments is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.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) 692-4220**	1-6-04	John W. Carlin

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 **1** 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
2/9/04	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 ITEM NO.	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)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	**Critical Infrastructure Information submissions** **See attached sheet.** c.c. Agency, NR, NWMW		

Department of Homeland Security (DHS)
Information Analysis and Infrastructure Protection (IAIP) Directorate
Critical Infrastructure Information Program

1. Critical Infrastructure Information[1] (CII) submissions received by DHS in all media and formats that **do not** meet the requirements for "Protected CII" contained in Section 214(e) of the Homeland Security Act of 2002.

   CII submissions consist of voluntarily submitted records or information concerning actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety. Submissions may identify and describe physical buildings, facilities or similar infrastructure, computers, computer systems, computer or communication networks, any component hardware or elements of computer systems, software programs, processing instructions, or information or data in transmission or storage devices in computer systems.

   AUTHORIZED DISPOSITION: Return to submitter if requested, or destroy within 30 calendar days of making the final non-protection determination in accordance with provisions found in 6 CFR Part 29, or when no longer needed for current business, whichever is later.

2. Email and word processing documents related to Non-Protected CII submissions

   a. Copies that have no further value after the recordkeeping copy is made, including copies maintained by individuals in personal files, personal electronic mail directories, or other directories on hard disk or network drives, and copies on shared networks that are used only to produce the recordkeeping copy.

   AUTHORIZED DISPOSITION: Delete/destroy within 180 days after the recordkeeping

---

[1] The Homeland Security Act of 2002 defines critical infrastructure information as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems— (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety; (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation "

copy has been produced.

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy.

AUTHORIZED DISPOSITION: Delete/destroy when dissemination, revision, and updating is complete.