REQUEST FOR RECORDS DISPOSITION AUTHORITY	LEAVE BLANK (NARA use only) JOB NUMBER N1-563-08-17
To: NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD, COLLEGE PARK, MID 20740-6001	Date Received 2-26-2008
1 FROM (Agency or establishment) **Department of Homeland Security**	NOTIFICATION TO AGENCY
2 MAJOR SUB DIVISION **National Protection and 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request, including amendments is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10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 **National Cyber Security Division (NCSD)**	

4 NAME OF PERSON WITH WHOM TO CONFER	5 TELEPHONE	DATE	ARCHIVIST OF THE UNITED STATES
Kathy Schultz	**202-447-5075**	7-3-2008	WITHDRAWN

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
2/21/08	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7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)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:** **National Cyber Security Division Program Records**		

U.S. Department of Homeland Security

Headquarters Records Schedules

National Cyber Security Division (NCSD)

The National Cyber Security Division seeks to protect the critical cyber infrastructure 24 hours a day, 7 days a week. The National Cyberspace Response System coordinates the cyber leadership, processes, and protocols that will determine when and what action(s) need to be taken as cyber incidents arise.

Through Cyber Risk Management, the National Cyber Security Division seeks to assess risk, prioritize resources, and execute protective measures critical to securing our cyber infrastructure

NCSD Records Schedules apply to all records generated or received in the course of NCSD business including mission records, which document the NCSD's performance of its mission functions, and administrative records, which are common to several or all government agencies (e.g., records relating to civilian personnel, fiscal accounting, procurement, communications, printing, and other common functions). They indicate the length of time the records within each record series are to be maintained in office areas, on personal computers, in central records centers or on servers, and when and if such series may be microfilmed, destroyed, or transferred to an archive. They also specify which records are temporary and which must be stored permanently. NCSD Records Schedules are developed by the NCSD Records Officer and staff in cooperation and are sent to the National Archives and Records Administration (NARA) to be approved by the Archivist of the United States

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

1 Communication and Distribution Strategy Files

Records contain communications and distribution plans used to document strategies to announce and disseminate NCSD information, publications, and reports. A communications plan is an internal NCSD document containing basic information on regulations, reports to Congress, and major policy statements and actions and the strategy for their communication to the affected communities and interested public. A distribution plan is an internal NCSD document containing basic information about publications and the strategies for public distribution. Files include copies of the communications and distribution plan (with latest comments), copies of the action or publication, transmittal memos and letters, copies fact sheets, copies of any press notifications

Disposition:

TEMPORARY. Cut off when superseded or obsolete. Destroy or delete 5 years after cutoff.

2 Customer Services Records

Reports which provide substantive input into consolidated NCSD reports generated by the NCSD and information used by the NCSD Executive Secretariat to respond to tasking

Disposition:

TEMPORARY. Cutoff at the end of the calendar year or when no longer needed for review and analysis, whichever is later. Destroy or delete 5 years after cutoff.

3 Cyber Security Standards and Best Practices and Research and Development Records

Records related to the development of cyber security standards, best practices, and research and development

Disposition:

TEMPORARY. Cutoff at the end of the calendar year or when no longer needed for review and analysis, whichever is later. Destroy or delete 3 years after cutoff.

4 HR Strategy Records

Record copy of employee satisfaction program file, including development of questionnaires, questionnaires, procedures for conduct of survey, status reports, and analysis of results

Disposition:

TEMPORARY. Cut off at completion of study. Destroy or delete 3 years after cutoff.

5 Key Asset and Critical Infrastructure Protection Program Files

Key Asset and Critical Infrastructure Protection consists of activities to determine risk to critical infrastructure including control systems, the IT sector, and other sectors. It comprises an inventory of critical functions of all sectors, threat scenarios, and consequence, threat, and vulnerability information:

Record copy of program files, including contracts for assistance, studies, development of questionnaires, procedures, weekly status reports, analysis of results, allocation formulas, and questionnaires

Disposition:

TEMPORARY. Cut off at the completion of assessment. Destroy or delete 7 years after cutoff.

6 Key Asset and Critical Infrastructure Protection Reports

Key Asset and Critical Infrastructure Protection consists of activities to determine risk to critical infrastructure including control systems, the IT sector, and other sectors. It comprises an inventory of critical functions of all sectors, threat scenarios, and consequence, threat, and vulnerability information.

Record copy of final report

Disposition:

PERMANENT. Cut off at the completion of assessment. Transfer to NARA 7 years after cutoff.

7 Program Monitoring Records

Includes records which relate to the on-going management of programs and routine projects within programs. Types of files include both mission and operational programs and may be maintained by one or more organizational units. Specific types of records include correspondence; memoranda; staff meeting records such as agendas, background papers, attendance lists, and meeting minutes or summaries; routine office procedures; and reports and data relating to general policy and program matters, oversight reviews, interagency activity, research and other similar materials. Also includes project control files showing assignments, progress, and completion of projects

Disposition:

TEMPORARY. Cut off at the end of the calendar year. Destroy or delete 7 years after cutoff.