# Request for Records Disposition Authority

(See Instructions on reverse)

**To: National Archives and Records Administration (NIR)**
**Washington, DC 20408**

1. From: (Agency or establishment)
U.S. Department of State

2. Major Subdivision
Bureau of Diplomatic Security

3. Minor Subdivision
Office of Computer Security

4. Name of Person with whom to confer
Tasha Thian

5. Telephone (include area code)
(202) 261-8424

**Leave Blank (NARA Use Only)**

Job Number: N1-059-07-11

Date Received: 7/24/07

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request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.

Date: 9/27/08

Archivist of the United States: Allen Weinstein

6. **Agency Certification**

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

☒ is not required ☐ is attached ☐ has been requested

| Signature of Agency Representative | Title | Date (mm/dd/yyyy) |
|---|---|---|
| Margaret G. Peppe Margaret G. Peppe | Deputy Director for IPS and Agency Records Officer | 7/18/2007 |

| 7. Item Number | 8. Description of Item and Proposed Disposition | 9. GRS or Superseded Job Citation | 10. Action taken (NARA Use Only) |
|---|---|---|---|
| | Schedule Attached | | |

# Office of Computer Security DS/SI/CS
# Records Disposition Schedule

**Monitoring and Incident Response Division (DS/CS/MIR)**

**1.** **Interagency Agreement File (MOAs and MOUs)**

**Description:** File contains copies of Interagency Agreements (MOAs) or Memorandums of Understanding (MOUs) with other U.S. Government agencies. Includes memorandums in support of MOAs or MOUs.

**Disposition:** Temporary. Destroy upon termination of MOA/MOU or when no longer needed.

**DispAuthNo:** Pending

**2.** **Computer Incident Response Team (CIRT) Standard Operating Procedures**

**Description:** Monitoring and incident standard operating procedures in electronic format since 2002 on a shared drive that are periodically revised. All division employees have access to the files which date from 2002.

**Disposition:** Temporary. Destroy when superseded or no longer needed, whichever is later.

**DispAuthNo:** Pending

**3.** **Response and Data Analysis Repository (RADAR) Application (Computer Security Incident Handling, Reporting, and Follow-up System)**

**Description:** An electronic computer security incident/event tracking and reporting system. Records arranged by post/office with a system generated ticket number and date. The system documents findings and conclusions. Incidents are categorized by level of severity and are identified as an incident (more severe) or an event. Includes emails related to an incident or an event. System maintained by IRM.

a. Incident – Identified as a higher level cyber threat.

**Disposition:** Temporary. Destroy/delete 5 years after incident.

**DispAuthNo:** Pending

~~**3.** **Response and Data Analysis Repository (RADAR) Application (Computer Security Incident Handling, Reporting, and Follow-up System)**~~

**Description:** An electronic computer security incident/event tracking and reporting system. Records arranged by post/office with a system generated ticket number and date. The system documents findings and conclusions. Incidents are categorized by level of severity and are identified as an incident (more severe) or an event. Includes emails related to an incident or

an event. System maintained by IRM.

b. paper – classified hardcopy (paper) incidents.

**Disposition:** Temporary. Destroy 5 years after incident.

**DispAuthNo:** Pending

**Evaluation and Verification Program (DS/CS/EV)**

**4. Regional Computer Security Officer (RCSO) Resource Reporting System/Maximo**

**Description:** a. An electronic files system related to maintaining the security of systems and data. The system analyzes network infrastructure in regards to compliance, vulnerability, countermeasures. Generates reports including computer security assessments, trip reports to IPost, Findings Report (statistics regarding number of vulnerabilities identified), travel scheduling to each post based determined by vulnerability identified for each post, equipment and management reports, and budget information. Large database controlled by IRM.

**Disposition:** Temporary. Destroy 5 years after security assessment or when superseded, whichever is later.

**DispAuthNo:** Pending

~~4.~~ **Regional Computer Security Officer (RCSO) Source Reporting System**

**Description:** ~~b.~~ System Backup

A mirrored system of itself to another system. The back-up system is on another drive in an adjacent system. Utilizes RAID 5 backup system.

**Disposition:** Temporary. Delete/Destroy backup when second subsequent backup is verified as successful or when no longer needed for system restoration which is later.

**DispAuthNo:** GRS 20, Item 8 (b)

**5. Regional Computer Security Officer (RCSO) Standard Operating Procedures (SOPs)**

**Description:** Includes files regardless of media, related to SOPs' on training equipment, documentation, vendor support for equipment, work requirements by Region.

**Disposition:** Temporary. Destroy when superseded or no longer needed, whichever is later.

**DispAuthNo:** Pending

**6. Computer Security Configuration Documents**

**Description:** File contains records created and retained from detailed security analysis of hardware and software. Also copies of the standards and guidelines for departmental implementation of information technology hardware and software applications. Files maintained electronically.

**Disposition:** Temporary. Cut off at end of calendar year. Destroy 5 years after cut off or when certification is no longer needed, whichever is later.

**DispAuthNo:** Pending

**7. Regional Computer Security Officer (RCSO) Training Files**

**Description:** Files, regardless of media, are maintained by name of employee and includes training certificates, travel, and funding. Files used as performance matrix for reporting and tracking purposes.

**Disposition:** Temporary. Cut off at end of fiscal year. Destroy 10 years after cut off.

**DispAuthNo:** Pending

**Enterprise Technology, Policy, and Awareness Division (DS/CS/ETPA)**

**8. Cyber Security Awareness Program – Subject File**

**Description:** Contains informational and educational materials; brochures; general correspondence; memorandums; publications; speeches; telegrams dealing with cyber security awareness.

**Disposition:** Temporary. Cut off at end of calendar year. Destroy 5 years after cut off.

**DispAuthNo:** Pending

**9. Cyber Security Awareness Briefing Files**

**Description:** Files contain briefing material, regardless of media, cyber security awareness program including PowerPoint slides and videos.

**Disposition:** Temporary. Destroy 3 years after briefing or when superseded, whichever is later.

**DispAuthNo:** Pending.

**10. Cyber Security Awareness Training Course**

**Description:** On-line course for annual certification of cyber security training for OpenNet users. The database contains copies of the completion certificates with the OpenNet users name, office and date completed.

**Disposition:** Temporary. Destroy 3 years after course or when superseded or no longer needed, whichever is later.

**DispAuthNo:** Pending

**11. Overseas Security Policy Board (OSPB) Information Systems Security Working Group (ISSWG)**

**Description:** Records, regardless of media, documenting the accomplishments of OSPB ISSWG maintained by Department as OSPB ISSWG chair. Records relating to: establishment, organization, membership, and policy of OSPB; and records created by OSPB ISSWG: agenda, minutes, final reports, and related records documenting the accomplishments of OSPB ISSWG. Records maintained electronically.

**Disposition:** Temporary. Destroy 10 years after working group meeting or when no longer needed, whichever is later.

**DispAuthNo:** Pending

**12. Exception/Waiver Files**

**Description:** Files contain memorandums, telegrams and correspondence requesting recommendations and approval of exceptions to the Department's computer, communications and network security policies.

**Disposition:** Temporary. Destroy 5 years after final decision or when no longer needed, whichever is later.

**DispAuthNo:** Pending

**13. Committee on National Security Systems (CNSS) Files**

**Description:** File contains correspondence regarding the Department's position on national-level classified computer and communications security policies. The file also contains the voting results of the CNSS representatives which maintained by vote number.

**Disposition:** Temporary. Destroy 5 years after CNSS policy/instruction published.

**DispAuthNo:** Pending

**Cyber Threat Analysis Division (DS/CS/CTA)**

**14. Penetration Testing Reports**

**Description:** Records created and retained as a result of penetration testing to validate security posture and the integrity of departmental offices and computer network. The reports included but not limited to the Executive Summary and Detailed Technical Report maintained electronically.

**Disposition:** Temporary. Cut off at end of calendar year. Destroy 10 years after cut off or when superseded or obsolete, whichever is later.

**DispAuthNo:** Pending

**15. Daily Read Files**

**Description:** The file contains daily highlights, excerpts of reports and analysis of cyber issues that are of interest to the U.S. Government. Maintained electronically.

**Disposition:** Temporary. Cut off at end of calendar year. Destroy 10 years after point of distribution or when no longer needed, whichever is sooner.

**DispAuthNo:** Pending

**16.** **Cyber Threat Analysis Division (CTAD) Reports**

**Description:** The file contains information that is collected, analyzed, and disseminated on cyber threat intelligence gathered through open, proprietary, and collateral sources used to generate an assortment of reports to assist operational managers and policy makers with timely and relevant intelligence and to assist them in mitigating the cyber threat confronting the Department. Reports generated include but not limited to: Country Cyber Threat Assessments; Special Focus Reports; Computer Security Profiles and any other ad hoc reports.

**Disposition:** (a) Record copy (paper).

PERMANENT. Cut off at end of calendar year. Retire to RSC 10 years after cut off. Transfer to National Archives in 5 year blocks 25 years after cut off of most recent records in the block.

**DispAuthNo:** Pending

~~16.~~ **Cyber Threat Analysis Division (CTAD) Reports**

~~Description:~~ The file contains information that is collected, analyzed, and disseminated on cyber threat intelligence gathered through open, proprietary, and collateral sources used to generator an assortment of reports to assist operational managers and policy makers with timely and relevant intelligence and to assist them in mitigating the cyber threat confronting the Department. Reports generated include but not limited to: Country Cyber Threat Assessments; Special Focus Reports; Computer Security Profiles and any other ad hoc reports.

**Disposition:** (b) All other copies (paper or electronic).

TEMPORARY. Destroy when no longer needed.

**DispAuthNo:** Non-record

**17.** **Cyber Threat Analysis Division (CTAD) Quarterly Reports**

**Description:** The file contains reports generated by the Technical Analysis Special Operations Branch (TASOB) providing overall analysis regarding CTAD activities including but not limited to briefing information and statistical reporting. Maintained electronically.

**Disposition:** Temporary. Cut off at end of calendar year. Destroy 10 years after point of distribution or when no longer needed, whichever is later.

**DispAuthNo:** Pending

**18.** **Technical Analysis Special Operations Branch (TASOB) Reports**

**Description:** Records created and retained in collecting, analyzing, and reporting on security incidents, identifying potential threats and abnormalities within the network, profile malicious code including unauthorized modifications and activities on the DOS global information networks. Reports include but not limited to: Security Incident Reports; Technical Network Analysis; Postmortem Hard Drive Analysis and any other ad hoc reports.

**Disposition:** Temporary. Cut off at end of calendar year. Destroy 10 years after cut off or when no longer needed, whichever is later.

**DispAuthNo:** Pending