

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 <i>NI-05907-11</i>	
Date Received <i>7/24/07</i>	
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request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.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 <i>9/23/08</i>	Archivist of the United States <i>Allen Wank</i>

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 _____ page(s) are not now needed 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 of the GAO Manual for Guidance of Federal Agencies:

is not required is attached has been requested

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

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 GRS or Superseded Job Citation	10.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

(6/12/08)

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 Destroy when superseded or no longer needed, whichever is later.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

REQUEST FOR RECORDS DISPOSITION AUTHORITY (See Instructions on reverse)		LEAVE BLANK (NARA use only)	
TO: NATIONAL ARCHIVES and RECORDS ADMINISTRATION (NIR) WASHINGTON, DC 20408		JOB NUMBER NI-59-94-43	DATE RECEIVED 3/8/96
1. FROM (Agency or establishment) Department of State		NOTIFICATION TO AGENCY	
2. MAJOR SUBDIVISION Bureau of [REDACTED] Diplomatic Security		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 [REDACTED]			
4. NAME OF PERSON WITH WHOM TO CONFER John A. Cruce	5. TELEPHONE 202-647-7123	DATE 5-9-96	ARCHIVIST OF THE UNITED STATES <i>John W. Paul</i>
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 <u>53</u> page(s) are not now needed 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 of the GAO Manual for Guidance of Federal Agencies, <input type="checkbox"/> is not required; <input checked="" type="checkbox"/> is attached; or <input type="checkbox"/> has been requested.			
DATE 2/20/96	SIGNATURE OF AGENCY REPRESENTATIVE <i>Kenneth Rossman</i>	TITLE Records Officer, Department of State	

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
	[REDACTED]		

Board B

93. Overseas Security Policy ~~Group~~ File (OSP~~G~~).

Correspondence, memorandums, and other documentation on interagency overseas security policies covering agendas, assistance, committees, interagency cooperation, issues, liaison, membership, minutes (drafts and finals), policies, security, standards handbook, talking points, working groups, and other related subjects.

- a. Records relating to: establishment, organization, membership, and policy of OSP~~G~~; and records created by OSPG: agenda, minutes, final reports, and related records documenting the accomplishments of OSP~~G~~ maintained by Department as OSP~~G~~ chair.

Arrange file by TAGS and Terms.

Cut off file at end of each calendar year.

Volume on hand: 1 box. Annual volume: 1 box.

Disposition: Permanent. Retire to RSC 3 years after cut off date for transfer to WNRC. Transfer to National Archives 30 years after cut off date.

- b. All other OSPG records.

Disposition: Destroy 3 years after cut off date or when no longer needed for reference, whichever is sooner.

{96} **Privacy Act General - Administrative File.** These records are covered by GRS 14, Item 26 and are not under appraisal here.

{97} **Privacy - Case File.** The Office of Freedom of Information, Privacy, and Classification Review (A/IM/IS/FPC) is responsible for maintaining the Department's official Privacy Act files and follows the requirements of GRS 14. This item covers the copies of relevant material maintained by DS in its files. Copies of requestor's letters, the Department's response and the documentation on the search are made a part of the individual's file and will be disposed of in accordance with the disposition for those files. The other material may include copies of the information noted above as well as other routine and facilitative material. I recommend approval of the destruction of those records.

⁹³
{98} **Overseas Security Policy Board (OSPB).** This item covers the records of the Overseas Security Policy Board, the follow-on organization to the Overseas Security Policy Group. The title will be changed on the final schedule. The OSPB is an inter-agency group responsible for establishing and clearing policies and procedures concerning overseas security matters. The Department of State serves as the chair and executive secretary of the Board. The remaining membership consists of representatives of AID, DIA, the Department of Commerce, the Department of the Treasury, NSA, the Peace Corps, the Foreign Agricultural Service, NASA, OMB, CIA, FBI, the Department of Justice, the Department of Transportation, USIA, FAA, ACDA, and the DCI Center for Security Evaluation. The OSPB reports to the President through the NSC, although there are no formal reporting requirements.

Before final approval of this schedule, this item should be moved to the section of the schedule covering DS/DSS. The Department has divided this item into two sub-items. I recommend approval of these two sub-items. Item 98(a) covers the basic background and policy documentation relating to the OSPB. These records clearly warrant eventual transfer to the National Archives. Before final approval, I recommend that the description of the types of records covered by this sub-item be revised to read: "all agendas; minutes; drafts of policies, standards or agreements circulated for approval; all responses from members to drafts; any handouts presented at regular meetings; and all other documents relating to the operations of the Board." This language comes from the Board charter which mandates that the Department preserve those records. Item 98(b) covers all other OSBP records, which in this case means the non-substantive

routine and facilitative material relating to meeting time and places. These records do not warrant preservation.

{99} **Security Planning - Program File.** This item covers records relating to security planning within the Department. The files include correspondence, memorandums, reports, charts, plans, proposals, budget information, and other documentation relating to goals and objectives of the security program, systems and operations planning, vulnerabilities, program requirement, and other related matters.

I recommend approval of this item. These records do not warrant preservation in the National Archives. While they are the basic DS planning files covering the Department security program, the key documentation will also be found among the files covered by Item which are recommended for permanent retention, as well as other permanent files of the Department. I do not believe that it is necessary to keep these files, too.

{100} **Security Policy Publications File.** The records covered by this item deal with the preparation on clearance of all major Departmental regulations, standards, and issuance relating to security matters. In addition to a record set of the publications, the files include all relevant documentation relating to the development of those policies. I recommend approval of this item. The Department has divided this item into two sub-items. Item 100 (a) covers the master set and clearly warrant eventual transfer to the National Archives. These permanent records will also include the background documentation. Item 100 (b) covers all other copies.

{101} **Security Grant Case Files.** This item covers the files on security-related grants administered by the Bureau of Diplomatic Security. The grants program began in 1990 and covers grants relating to two major areas of security training: (1) training for foreign police officials and (2) grants to american cities for the "extraordinary" protection of diplomats and foreign missions in the U.S. Under the first heading, there are two large grants/cooperative agreements. The first is with the Louisiana State Policy Academy to provide training **facilities** used in training foreign police officials. The second is with the Louisiana State University to provide the trainers and the training. A third, much smaller, arrangement with the Connecticut State Police to train explosive-detecting dogs, is in the process of ending. Under the second heading is a program begun in 1984 with an MOU with the New York City Police Department under which the Department provided funds to pay for extra police for extraordinary occasions. Over time, this

From: "Michael Churgin" <MChurgin@law.utexas.edu>
To: "Jerome Nashorn" <jerome.nashorn@nara.gov>
Date: 9/5/2008 2:35:58 PM
Subject: comments on proposed schedules

N1-059-07-11

#11 There is a reference in the appraisal that the records of the Executive Secretariat is a better source, but there is no indication of an approved schedule nor an indication of the period that the records are preserved in that set of records.

Best.

Michael

=====

Michael J. Churgin	(512) 232 - 1330
University of Texas School of Law	FAX: 512.471.6988
727 East Dean Keeton Street	
Austin, Texas 78705	mchurgin@mail.law.utexas.edu

August 7, 2008

Professor Michael J. Churgin
University of Texas School of Law
727 East Dean Keeton Street
Austin, TX 78705

Dear Michael:

This is in response to your request of July 28, 2008, for copies of proposed disposition schedules and appraisal memorandums for Disposition Jobs N1-59-07-11, N1-59-08-2, N1-59-08-5, N1-59-08-8, N1-60-08-11, N1-145-05-1, N1-145-05-2, N1-255-07-2, and N1-406-08-3 for which notice of availability was published in the *Federal Register*.

Enclosed are copies of proposed disposition schedules and appraisal memorandums for Disposition Jobs N1-59-07-11, N1-59-08-2, N1-59-08-5, N1-59-08-8, N1-60-08-11, N1-145-05-1, N1-145-05-2, N1-255-07-2, and N1-406-08-3. Comments concerning these schedules must be received 30 days from the date of this letter.

Sincerely,

JEROME NASHORN
Supervisor
Life Cycle Management Division

Enclosures

S:\FedReg\Requestors\Churgin\FY08\CHUR80806
File:Federal Register Documentation File 1311.1b

Official File – NWML
Reading File – NWML
Roberson
Sears

N1-59-07-11 Fischer
N1-59-08-2 Fischer
N1-59-08-5 Fischer
N1-59-08-8 Langbart
N1-60-08-11 Fairbank
N1-145-05-1 Carter
N1-145-05-2 Carter
N1-255-07-2 Hulmston
N1-406-08-3 Lipford
lr/sg/08/06/08

From: "Michael Churgin" <MChurgin@law.utexas.edu>
To: <requestschedule@nara.gov>
Date: 7/28/2008 5:54:06 PM
Subject: request for appraisals and proposed schedules

May I please see the appraisal and proposed schedule for the following:

- N1-145-05-1 -- Ag
- N1-145-05-2 -- Ag
- N1-60-08-11 -- DOJ
- N1-59-07-11 -- State
- N1-59-08-8 -- State
- N1-59-08-2 -- State
- N1-59-08-5 -- State
- N1-406-08-3 -- DOT-FHA
- N1-255-07-2 -- NASA

My address is below. Thank you.

MJChurgin

=====

Michael J. Churgin (512) 232-1330
University of Texas School of Law (fax)(512) 471-6988
727 East Dean Keeton Street mchurgin@mail.law.utexas.edu
Austin, Texas 78705

July 14, 2008

Ms. Patrice McDermott
OpenTheGovernment.org
1742 Connecticut Avenue, N.W., 3rd Floor
Washington, DC 20009

Dear Ms. McDermott:

This is in response to your request of July 2, 2008, for copies of the proposed disposition schedules and appraisal memorandums for Disposition Jobs N1-59-07-11, N1-60-08-15, and N1-65-08-9 for which notice of availability was published in the *Federal Register*.

Enclosed are copies of Disposition Jobs and appraisal memorandums for N1-59-07-11 and N1-60-08-15. Comments concerning this schedule must be received 30 days from the date of this letter.

We have not completed processing the remaining schedule you requested, (N1-65-08-9). Upon completion we will send you this job and you will have 30 days to submit comments.

Sincerely,

JEROME NASHORN
Supervisor
Life Cycle Management Division

Enclosures

S:\FedReg\Requestors\Others\McDermott080714
File:Federal Register Documentation File 1311.1b

Official File – NWML
Reading File – NWML
Roberson
Sears

N1-59-07-11 Fischer
N1-60-08-15 Fairbank
N1-65-08-9 Cooper

LR/sg/07/14/08

July 14, 2008

Mr. Greg Nojeim
Center for Democracy & Technology
1634 Eye Street, N.W., #1100
Washington, DC 20006

Dear Mr. Nojeim:

This is in response to the request made on your behalf by Patrice McDermott of July 2, 2008, for copies of the proposed disposition schedules and appraisal memorandums for Disposition Jobs N1-59-07-11, N1-60-08-15, and N1-65-08-9 for which notice of availability was published in the *Federal Register*.

Enclosed are copies of Disposition Jobs and appraisal memorandums for N1-59-07-11 and N1-60-08-15. Comments concerning this schedule must be received 30 days from the date of this letter.

We have not completed processing the remaining schedule you requested, (N1-65-08-9). Upon completion we will send you this job and you will have 30 days to submit comments.

Sincerely,

JEROME NASHORN
Supervisor
Life Cycle Management Division

Enclosures

S:\FedReg\Requestors\Others\Graves080714
File:Federal Register Documentation File 1311.1b

Official File – NWML
Reading File – NWML
Roberson
Sears

N1-59-07-11: Fischer
N1-60-08-15 Fairbank
N1-65-08-9 Cooper

LR/sg/07/14/08

July 14, 2008

Ms. Lisa Graves
Center for National Security Studies
1120 19th Street, N.W., 8th Floor
Washington, DC 20036

Dear Ms. Graves:

This is in response to the request made on your behalf by Patrice McDermott of July 2, 2008, for copies of the proposed disposition schedules and appraisal memorandums for Disposition Jobs N1-59-07-11, N1-60-08-15, and N1-65-08-9 for which notice of availability was published in the *Federal Register*.

Enclosed are copies of Disposition Jobs and appraisal memorandums for N1-59-07-11 and N1-60-08-15. Comments concerning this schedule must be received 30 days from the date of this letter.

We have not completed processing the remaining schedule you requested, (N1-65-08-9). Upon completion we will send you this job and you will have 30 days to submit comments.

Sincerely,

JEROME NASHORN
Supervisor
Life Cycle Management Division

Enclosures

S:\FedReg\Requestors\Others\Graves080714
File:Federal Register Documentation File 1311.1b

Official File – NWML
Reading File – NWML
Roberson
Sears

N1-59-07-11 Fischer
N1-60-08-15 Fairbank
N1-65-08-9 Cooper

LR/sg/07/14/08

From: "Patrice McDermott" <pmcdermott@openthegovernment.org>
To: <requestschedule@nara.gov>
Date: 7/2/2008 10:09:27 AM
Subject: schedules & appraisal reports requested

Please send the records schedules and appraisal reports for:
9. Department of Justice, Criminal Division (N1-60-08-15, 1 item, 1 temporary item).

12. Department of Justice, Federal Bureau of Investigation (N1-65-08-9, 3 items, 3 temporary items).

15. Department of State, Bureau of Diplomatic Security (N1-59-07-11, 19 items, 18 temporary items).

to

Patrice McDermott
1742 Connecticut Avenue N.W., 3rd Floor
Washington, D. C. 20009

Lisa Graves
Center for National Security Studies
1120 19th Street, NW
8th Floor
Washington, DC 20036

Greg Nojeim
Center for Democracy & Technology
634 Eye Street NW #1100
Washington DC, 20006.

Thank you.
Patrice McDermott, Director
OpenTheGovernment.org
www.openthegovernment.org
202.332.OPEN (6736)

CC: <gnojeim@cdt.org>, "Lisa Graves" <lgraves@cncs.org>

From: "Chichester, Lois S" <ChichesterLS@state.gov>
To: <William.Fischer@nara.gov>
Date: 6/12/2008 9:14:56 AM
Subject: FW: Status Request on DS/SI/CS schedules

Hi Bill,

Please see the attachment and let me know the next step required of our office. Have a good evening.

Regards, Lois

-----Original Message-----

From: Holland, Mary S
Sent: Wednesday, June 04, 2008 3:31 PM
To: Chichester, Lois S
Subject: FW: Status Request on DS/SI/CS schedules

Lois,

Attached you will find the February 6, 2008, memo I signed approving the NARA schedules. I hope that this will now conclude action on this section of the DS project. Please let me know if this is not the case.

msh

-----Original Message-----

From: Holland, Mary S
Sent: Tuesday, June 03, 2008 4:19 PM
To: Chichester, Lois S
Cc: Giamporcaro, Jeanne; Spruell, Mary; Siljegovic, Kathleen; Thian, Tasha M; Mapp, Mary L; Mapp, Mary L; Keene, Cooperine C
Subject: RE: Status Request on DS/SI/CS schedules

I am confident that I already approved the NARA schedules. Let me double check and get back to you. msh

-----Original Message-----

From: Chichester, Lois S
Sent: Tuesday, June 03, 2008 3:42 PM
To: Holland, Mary S
Cc: Giamporcaro, Jeanne; Spruell, Mary; Siljegovic, Kathleen; Thian, Tasha M
Subject: Status Request on DS/SI/CS schedules

Hi Mary Sue,

This is a status check on the DS/SI/CS' revised schedules sent to you for clearance which were forwarded to you by NARA:Bill Fischer on 1/29/08. ISS and NARA would like to conclude this section of the DS scheduling project.

Regards,

Lois S. Chichester
Lead Program Analyst
A/ISS/IPS-RA
(202) 663-2776, x3-2776
(202) 261-8586 (fax)
chichesterls@state.gov

You are invited to complete our Records Management Customer Satisfaction Survey at the following link:

<http://lm.a.state.gov/websurvey/index.cfm?fa-showSurvey&survey=2172>. We value your comments and thank you in advance for your assistance.

This e-mail is unclassified based upon the definitions provided in E.O. 12958

February 6, 2008

MEMORANDUM

To: DS/SI/CS – Mary Stone Holland, Director
DS/SI/CS – Nell Richardson

From: A/ISS/IPS - RA – Anita L. Boone

Subject: Appraisal of Job N1-59-07-11 for DS/SI/CS

The Appraisal Archivist has completed its appraisal for the DS/SI/CS, Office of Computer Security and has made some minor changes to the schedules. We have completed a review and discussion of these proposed recommended changes provided by NARA. However, there are some changes in the standard language on the original schedules that you will need to be made aware of. Please note that these items are listed as follows: Item 7, Cyber Security Awareness Briefing Files, Disposition: Destroy 3 years, Item 8, Cyber Security Awareness Training Course, Disposition: Destroy 3 years, Item 13, Penetration Testing Reports, Disposition: Destroy 10 years, Item 15, Cyber Threat Analysis Division (CTAD) Reports, Disposition: Permanent and Item 18, Regional Computer Security Officer (RCSO) Training Files, Disposition: Cut off at end of fiscal year. (See the attached e-mail dated 01/29/08) from Bill Fischer with the changes to the schedule.

We request DS/SI/CS clearance for resubmission of the schedules to the National Archives and Records Administration (NARA) for final approval.

Please have the DS/SI/CS Director to review the attached schedule to ensure that we have accurately incorporated your requested revision(s), sign this memo for concurrence. If you find the draft acceptable we request your clearance to resubmit the schedule to the National Archives and Records Administration (NARA) for approval.

DS/SI/CS Concurrs

Mary Stone Holland
Name
Director - Office of
Title *Computer Security*

Date *4/23/08*

Attachment: As stated

From: William Fischer
To: BooneAL@state.gov; Chichester, Lois S
Date: 1/30/2008 11:17:16 AM
Subject: NARA Job No. N1-59-07-11 (DS/Office of Computer Security)

January 30, 2008

Dear Lois and Anita:

NARA has completed its appraisal of Job No. N1-59-07-11 (DS/Office of Computer Security). Before this schedule can be signed, NARA recommends some minor changes to the schedule (see attached copy).

Since this schedule is arranged by component units of the Office of Computer Security, I also recommend that the numbering of the items on the final schedule be rearranged to reflect the organizational arrangement of the schedule.

The recommended changes include:

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

Item 2, Computer Incident Response Team (CIRT) SOPs.

I recommend that the disposition be as follows: "Destroy when superseded or no longer needed, whichever is later."

Item 19, RADAR Application.

I recommend that the title be changed to "Response and Data Analysis Repository (RADAR)."

I recommend that the disposition be as follows: "Destroy/delete 5 years after incident."

Item 20, RADAR Application.

I recommend that the title be changed to "Response and Data Analysis Repository (RADAR)."

I recommend that the disposition be as follows: "Destroy 5 years after incident."

Evaluation and Verification Program (DS/CS/EV)

Item 3, Regional Computer Security Officer (RCSO) Resource Reporting System.

I recommend that the disposition be as follows: "Destroy 5 years after security assessment or when superseded, whichever is later."

Item 4, Regional Computer Security Officer (RCSO) Resource Reporting System.

This item will be crossed off the schedule since it is covered by GRS 20, Item 8 (b).

Item 5, Regional Computer Security Officer (RCSO) SOPs.

I recommend that the disposition be as follows: "Destroy when superseded or no longer needed, whichever is later."

Item 12, Computer Security Configuration Documents.

I recommend that the disposition be as follows: "Cut off at end of calendar year. Destroy 5 years after cut off or when certification is no longer needed, whichever is later."

Item 18, Regional Computer Security Officer Training Files.

I recommend that the disposition be as follows: "Cut off at end of fiscal year. Destroy 10 years after cut off."

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

Item 6, Cyber Security Awareness Program – Subject File.

I recommend that the disposition be as follows: "Cut off at end of calendar year. Destroy 5 years after cut off."

Item 7, Cyber Security Awareness Briefing Files.

I recommend that the disposition be as follows: "Destroy 3 years after briefing or when superseded, whichever is later."

Item 8, Cyber Security Awareness Training Course.

I recommend that the disposition be as follows: "Destroy 3 years after course or when superseded or no longer needed, whichever is later."

Item 9, Overseas Security Policy Board (OSPB) Information Systems Security Working Group (ISSWG).

I recommend that the disposition be as follows: "Destroy 10 years after working group meeting or when no longer needed, whichever is later."

I recommend that the description for this item be revised to state that these records are media neutral.

Item 10, Exception/Waiver Files.

I recommend that the disposition be as follows: "Destroy 5 years after final decision or when no longer needed, whichever is later."

Item 11, Committee on National Security Systems (CNSS) Files.

I recommend that the disposition be as follows: "Destroy 5 years after CNSS policy/instruction published."

Cyber Threat Analysis Division (DS/CS/CTA)

Item 13, Penetration Testing Reports.

I recommend that the disposition be as follows: "Cut off at end of calendar year. Destroy 10 years after cut off or when superseded or obsolete, whichever is later."

Item 14, Daily Read Files.

I recommend that the disposition be as follows: "Cut off at end of calendar year. Destroy 10 years after point of distribution or when no longer needed, whichever is sooner."

Item 15, Cyber Threat Analysis Division (CTAD) Reports.

I recommend that the meaning of the acronym CTAD be spelled out in the title.

I recommend that the designation be changed from temporary to permanent and the disposition be as follows:

(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.

(b) All other copies (paper or electronic).

TEMPORARY. Destroy when no longer needed.

Item 16, Technical Analysis Special Operations Branch Quarterly Reports.

I recommend that the title be changed to Cyber Threat Analysis Division (CTAD) Quarterly Reports because the reports document the activities of the entire division, not just the Technical Analysis Special Operations Branch.

I recommend that the disposition be as follows: "Cut off at end of calendar year. Destroy 10 years after point of distribution or when no longer needed, whichever is later."

Item 17, Technical Analysis Special Operations Branch (TASOB) Reports.

I recommend that the meaning of the acronym TASOB be spelled out in the title.

I recommend that the disposition be as follows: "Cut off at end of calendar year. Destroy 10 years after cut off or when no longer needed, whichever is later."

Sincerely
William Fischer
Appraiser

WILLIAM P. FISCHER
Senior Records Analyst
NWML, Rm. 2100
National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740-6001
william.fischer@nara.gov
(301) 837-1907 (telephone)
(301) 837-3697 (fax)

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 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: (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: Pending

17. Description: **Cyber Threat Analysis Division (CTAD) Quarterly Reports**
 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. Description: **Technical Analysis Special Operations Branch (TASOB) Reports**
 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



National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

MH
12/18/07

Date: December 17, 2007
Appraiser: William Fischer, NWML
Agency: Department of State
Subject: Job. No. N1-59-07-11

INTRODUCTION

Schedule Overview

Bureau of Diplomatic Security (DS), Office of Computer Security (DS/SI/CS)

Administrative History

The Senior Coordinator for Security Infrastructure (SI) in the Bureau of Diplomatic Security manages the Department's overall strategy and planning in the area of information security, computer security, and personnel security. The Senior Coordinator created the Office of Computer Security to develop, formulate, recommend, and coordinate Department-wide cyber security infrastructure policy, standards, and guidelines. The Office of Computer Security accomplishes its program mission through four component units: 1) Monitoring and Incident Response Division; 2) Evaluation and Verification Program; 3) Enterprise Technology, Policy, and Awareness Division; and 4) Cyber Threat Analysis Division.

Additional Information

Since this schedule is arranged by component units of the Office of Computer Security, I recommend that the numbering of the items on the final schedule be rearranged to reflect the organizational arrangement of the schedule.

Overall Recommendation

I recommend approval with changes.

APPRAISAL

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

The Monitoring and Incident Response Division within the Office of Computer Security handles activities relating to the detection, response, and reporting on security threats against Department computer networks and information systems.

This section of the report covers Items 1-2 and 19-20.

Item 1, Interagency Agreement File (MOAs and MOUs).

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records are routine and facilitative in nature.

Adequacy of Proposed Retention Period(s) for temporary records: Adequate from the standpoint of legal rights and accountability.

Media Neutrality: Not Requested. Recordkeeping medium is paper.

Item 2, Computer Incident Response Team (CIRT) SOPs.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records are routine and facilitative in nature.

*Does not document significant actions of Federal officials.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. I recommend that the disposition be as follows: "Destroy when superseded or no longer needed, whichever is later."

Media Neutrality: Not Requested. Recordkeeping medium is electronic.

Item 3, RADAR Application (formerly Item 19).

I recommend that the title be changed to "Response and Data Analysis Repository (RADAR)." RADAR is a module within the Department's Universal Trouble Ticket system, a tracking system used to monitor technical problems reported to IT support units (e.g., computer help desk), used in the case of computer security incidents against Department networks. This item covers unclassified incident ticket data. Data includes the following types of information: unique ticket number, ticket status, priority level, ticket type, originating source, event date and time, event description, source of problem, computer hardware information, affected location, bureau, and country.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value.

*Does not document significant actions of Federal officials.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. I recommend that the disposition be as follows: "Destroy/delete 5 years after incident."

Media Neutrality: Not Requested. Recordkeeping medium is electronic.

Item 3, RADAR Application (formerly Item 20).

I recommend that the title be changed to "Response and Data Analysis Repository (RADAR)." This item covers classified incident tickets.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value.

*Does not document significant actions of Federal officials.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. I recommend that the disposition be as follows: "Destroy 5 years after incident."
Media Neutrality: Not Requested. Recordkeeping medium is paper.

Evaluation and Verification Program (DS/CS/EV)

The Evaluation and Verification Program within the Office of Computer Security conducts technical evaluations and verifications of Department networks and computer systems to ensure technical compliance with security standards.

This section of the report covers Items 3-5, 12 and 18.

Item 4a, Regional Computer Security Officer (RCSO) Resource Reporting System (formerly Item 3a).

This is a web-based information system used by RCSOs to manage and perform computer security assessments of Department networks and systems.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

* Has little or no research value. These data are of a technical nature and do not provide significant documentation about the computer security program.

*Does not document significant actions of Federal officials. These data do not provide a significant source of documentation about program policies, decisions, or actions.

Adequacy of Proposed Retention Period for temporary records: Inadequate. I recommend that the disposition be as follows: "Destroy 5 years after security assessment or when superseded, whichever is later."

Media Neutrality: Not Requested. Recordkeeping medium is electronic.

Item 4b, Regional Computer Security Officer (RCSO) Resource Reporting System (formerly Item 3b). 4

This item will be crossed off the schedule since it is covered by GRS 20, Item 8 (b).

Item 5, Regional Computer Security Officer (RCSO) SOPs.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records are routine and facilitative in nature.

*Does not document significant actions of Federal officials.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. I recommend that the disposition be as follows: "Destroy when superseded or no longer needed, whichever is later."

Media Neutrality: Requested and Approved.

Item 6, Computer Security Configuration Documents (formerly Item 12).

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records consist of computer security technical standards and guidelines and do not provide significant documentation about the computer security program.

*Does not document significant actions of Federal officials. These records are based on National Institute for Science and Technology security standards and do not provide unique information about the computer security program.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. In order to protect legal rights and accountability, I am proposing that the retention period and disposition instructions be as follows: "Cut off at end of calendar year. Destroy 5 years after cut off or when certification is no longer needed, whichever is later."

Media Neutrality: Not Requested. Recordkeeping medium is electronic.

Item 7, Regional Computer Security Officer Training Files (formerly Item 18).

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Recordkeeping copy approved as temporary. NARA Job No. N1-59-07-1, Item 6.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. I recommend that the disposition be as follows: "Cut off at end of fiscal year. Destroy 10 years after cut off."

Media Neutrality: Requested and Approved.

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

The Enterprise Technology, Policy, and Awareness Division within the Office of Computer Security handles issues relating to computer security technical standards and guidelines.

This section of the report covers Items 6-11.

Item 8, Cyber Security Awareness Program – Subject File (formerly Item 6).

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records provide documentation of standard computer security issues tailored to the Department.

*Does not document significant actions of Federal officials.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. I recommend that the disposition be as follows: "Cut off at end of calendar year. Destroy 5 years after cut off."

Media Neutrality: Not Requested. Recordkeeping medium is paper.

Item 9, Cyber Security Awareness Briefing Files (formerly Item 7).

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records provide documentation of standard computer security issues tailored to the Department.

*Does not document significant actions of Federal officials.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. In order to protect legal rights and accountability, I am proposing that the retention period and disposition instructions be as follows: "Destroy 3 years after briefing or when superseded, whichever is later."

Media Neutrality: Requested and Approved.

Item 10, Cyber Security Awareness Training Course (formerly Item 8).

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records are routine and facilitative in nature.

*Does not document significant actions of Federal officials.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. In order to protect legal rights and accountability, I am proposing that the retention period and disposition instructions be as follows: "Destroy 3 years after course or when superseded or no longer needed, whichever is later."

Media Neutrality: Not Requested. Recordkeeping medium is electronic.

Item 11, Overseas Security Policy Board (OSPB) Information Systems Security Working Group (ISSWG) (formerly Item 9).

The Policy and Planning Division within the Office of the Executive Director for Diplomatic Security serves as the Executive Secretariat for the OSPB, an interagency consultative body that considers, develops, coordinates, and promotes security policies, standards, and agreements on overseas security programs. The Executive Secretariat coordinates all activities of the OSPB, the working group standards development activities, and assists in the resolution of disagreements between agencies. The Office of Computer Security leads the ISSWG under the direction of the Executive Secretariat.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records do not provide a highly usable source of information about the development of computer security standards.

*Does not document significant actions of Federal officials. The Executive Secretariat for the OSPB is the best source of documentation for significant Federal deliberations and actions relating to computer security technical standards and policies, including matters relating to the proceedings of the ISSWG.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. I recommend that the disposition be as follows: "Destroy 10 years after working group meeting or when no longer needed, whichever is later."

Media Neutrality: Not Requested. Recordkeeping medium is electronic and paper. I recommend that the description for this item be revised to state that these records are media neutral.

Item 12, Exception/Waiver Files (formerly Item 10).

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records are routine and facilitative in nature.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. I recommend that the disposition be as follows: "Destroy 5 years after final decision or when no longer needed, whichever is later."

Media Neutrality: Not Requested. Recordkeeping medium is paper.

Item 13, Committee on National Security Systems (CNSS) Files (formerly Item 11).

The Department of Defense chairs the CNSS.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records do not provide a significant source of information about the development of computer security technical standards or policy for classified systems.

*Does not document significant actions of Federal officials. Although these records document the Department's position on technical security standards for classified automated information systems and networks, the Chair of the CNSS is the best source of documentation for significant Federal decisions and actions relating to the proceedings of the CNSS.

Adequacy of Proposed Retention Period(s) for temporary records: Inadequate. I recommend that the disposition be as follows: "Destroy 5 years after CNSS policy/instruction published."

Media Neutrality: Not Requested. Recordkeeping medium is electronic.

Cyber Threat Analysis Division (DS/CS/CTA)

The Cyber Threat Analysis Division within the Office of Computer Security conducts research and analysis and distributes information about cyber threats against the Department's computer networks and information systems.

This section of the report covers Items 13-17.

Item 14, Penetration Testing Reports (formerly Item 13).

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These reports are of a technical nature and do not provide unique or significant documentation about the computer security program.

*Does not document significant actions of Federal officials. These records do not provide a good source of documentation about program policies, decisions, or actions.

Adequacy of Proposed Retention Period for temporary records: Inadequate. In order to protect legal rights and accountability, I am proposing that the retention period and disposition instructions be as follows: "Cut off at end of calendar year. Destroy 10 years after cut off or when superseded or obsolete, whichever is later."

Media Neutrality: Not Requested. Recordkeeping medium is electronic.

Item 15, Daily Read Files (formerly Item 14).

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These records consist of routine announcements used to alert the Department and other government agencies about current cyber threats and do not provide unique or significant documentation about the computer security program.

*Does not document significant actions of Federal officials. These records do not provide a good source of documentation about program policies, decisions, or actions.

Adequacy of Proposed Retention Period for temporary records: Inadequate. In order to protect legal rights and accountability, I am proposing that the retention period and disposition instructions be as follows: "Cut off at end of calendar year. Destroy 10 years after point of distribution or when no longer needed, whichever is sooner."

Media Neutrality: Not Requested. Recordkeeping medium is electronic.

Item 16, Cyber Threat Analysis Division (CTAD) Reports (formerly Item 15).

I recommend that the meaning of the acronym CTAD be spelled out in the title.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Requires Change

Recommended Disposition: Permanent

Appraisal Justification:

*High potential research value. These records provide significant documentation about foreign cyber threats and capabilities and contribute substantially to an awareness and understanding of the nature of cyber warfare/terrorism.

*Documents significant actions of Federal officials. These records provide significant evidence of the Department's response to cyber threats.

Adequacy of Proposed Transfer Instructions: Requires Change. Since the agency originally proposed temporary, transfer instructions will have to be worked out with the agency. I am proposing that the disposition instructions be as follows:

(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.

(b) All other copies (paper or electronic).

TEMPORARY. Destroy when no longer needed.

Media Neutrality: Not Requested.

Item 17, Technical Analysis Special Operations Branch Quarterly Reports (formerly Item 16).

I recommend that the title be changed to Cyber Threat Analysis Division (CTAD) Quarterly Reports because the reports document the activities of the entire division, not just the Technical Analysis Special Operations Branch.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate.

Appraisal Justification:

*Has little or no research value. These reports do not provide unique or significant documentation about the computer security program. These reports merely provide a summarized account of quarterly program activities such as penetration tests (Item 14), daily read files (Item 15), special reports (Item 16), and other technical reports (Item 18) that does not add to a proper understanding of the computer security program. The quarterly reports do not add to the value of the information found in the records relating to the above referenced items.

*Does not document significant actions of Federal officials. These records do not provide a significant source of documentation about program policies, decisions, or actions.

Adequacy of Proposed Retention Period for temporary records: Inadequate. In order to protect legal rights and accountability, I am proposing that the retention period and disposition instructions be as follows: "Cut off at end of calendar year. Destroy 10 years after point of distribution or when no longer needed, whichever is later."

Media Neutrality: Not Requested. Recordkeeping medium is electronic.

Item 18, Technical Analysis Special Operations Branch (TASOB) Reports (formerly Item 17).

I recommend that the meaning of the acronym TASOB be spelled out in the title.

Proposed Disposition: Temporary

Appropriateness of Proposed Disposition: Appropriate

Appraisal Justification:

*Has little or no research value. These reports are of a technical nature and do not provide unique or significant documentation about the computer security program. They merely document routine technical inspections performed on Department networks and systems.

*Does not document significant actions of Federal officials. These records do not provide a significant source of documentation about program policies, decisions, or actions.

Adequacy of Proposed Retention Period for temporary records: Inadequate. In order to protect legal rights and accountability, I am proposing that the retention period and disposition instructions be as follows: "Cut off at end of calendar year. Destroy 10 years after cut off or when no longer needed, whichever is later."

Media Neutrality: Not Requested. Recordkeeping medium is electronic.

A handwritten signature in black ink that reads "Wm P Fischer". The signature is written in a cursive style with a large initial "W" and "F".

WILLIAM FISCHER
Appraiser

**REQUEST FOR STAKEHOLDER UNIT ACTION:
INFORMAL REVIEW OF APPRAISAL REPORT**

Job Number: N1-59-07-11

MRH 12/24/07

ROUTE TO: NWME	DATE SENT: <i>12/21/07</i>	DATE RECEIVED: JAN -2 2008
	DATE DUE TO SENDER: <i>1/16/07</i>	DATE RECEIVED BY SENDER:

MRH 01/28/08

FOR STAKEHOLDER USE. This job is transmitted for review of the appraisal report.

Concur: Date: *1/24/08* Signature: *Margaret Heil Adams*

Comment: _____

Do Not Concur: Date: _____ Signature: _____

Comment: _____

Contact: Bill Fischer (NWML) Tel. No. 301-837-1907

APPRAISER'S COMMENTS:

<p align="center">USE THIS FOR CONCURRENCES, APPROVALS, CLEARANCES, OR OTHER SIMILAR ACTIONS. ATTACH ADDITIONAL FORMAL COMMENTS IF NEEDED.</p>
--



National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: January 22, 2008
To: Bill Fischer, NWML
From: Greg LaMotta, NWME
Subject: N1-059-07-11 Bureau of Diplomatic Security: Office of Computer Security

Thanks for the opportunity to review the proposed schedule and appraisal report for the Bureau of Diplomatic Security's Office of Computer Security. In our Stakeholder Unit review of the schedule we had noted that Item 15, the Cyber Threat Analysis Division (CTAD) Reports may be permanent. Your appraisal report agrees with this assessment and asks that the proposed temporary retention be changed to permanent. Your report also suggests that the paper version of the reports be designated as the record copy. If this suggestion is approved, NWME will have no further comment on the schedule.

However, NWME would like to be notified if, at this time, or in the future, the electronic versions of the reports are designated as the record copy.

Greg LaMotta
Archives Specialist
Electronic and Special Media Records Services Division (NWME)

Concurrence: Margaret O'Neill Adams 1/24/08
Margaret O'Neill Adams Date
Manager, Archival Services
Electronic and Special Media Records Services Division (NWME)

Concurrence: Michael Carlson 1/24/08
Michael Carlson, Director Date
Electronic and Special Media Records Services Division (NWME)

REQUEST FOR STAKEHOLDER UNIT ACTION

Job No. N1-59-07-11

Date sent: 8/6/07

Date received: AUG 07 2007

Return to sender by: 8/13/07

m-r-h 08/27/07

Route To: (CIRCLE APPROPRIATE STAKEHOLDER)
1. NWME; <u>NWMW</u>; NWMD; NWCS; NWCT; NWCTC; NWCTM; NWCTF; NWCTB; NWL; NR
Return to: William Fischer, NWML, 2100, A2

- A. This Job has also been sent to: **NWME**; NWMW; **NWMD**; NWCS; **NWCTC**; NWCTM; NWCTF; NWCTB; NWL; NR; NWCT
- B. NWML general comments on this job:
- C. NWML wishes assistance in appraising these records:

FOR STAKEHOLDER USE. Check and fill out the line that applies.

1. Waives informal review. wants / ___ does not want to receive completed job.
- ___ 2. Wishes to review appraisal report. ___ wants/ ___ does not want to receive completed job.
- ___ 3. Wishes to participate directly in the appraisal of the entire job or the following selected items: _____ . SHU point of contact for appraisal is _____ - phone no. _____ .

SHU comments: *1) cft would be helpful to spell out ~~some~~ acronyms.*
2) do State prepared to maintain and migrate the "keep until no longer needed" items (such as 14, 16 and 17) for as long as they deem to want the records.

Date Sent: 8/23/07

SHU Signature Addie M. Compton

NWML Contact: William P. Fischer, NWML	Room number: 2100
	Phone No.: 301-837-1907

REQUEST FOR STAKEHOLDER UNIT ACTION

Job No. N1-59-07-11

Date sent: 8/6/07

Date received: 8/9/07

Return to sender by: 8/13/07

MRH 0812/07

Route To: (CIRCLE APPROPRIATE STAKEHOLDER)
1. <u>NWME; NWMW; NWMD; NWCS; NWCT; NWCTC; NWCTM; NWCTF; NWCTB; NWL; NR</u>
Return to: William Fischer, NWML, 2100, A2

- A. This Job has also been sent to: NWME; NWMW; NWMD; NWCS; NWCTC; NWCTM; NWCTF; NWCTB; NWL; NR; NWCT
- B. NWML general comments on this job:
- C. NWML wishes assistance in appraising these records:

FOR STAKEHOLDER USE. Check and fill out the line that applies.

1. Waives informal review. wants / does not want to receive completed job.
2. Wishes to review appraisal report. wants / does not want to receive completed job.
3. Wishes to participate directly in the appraisal of the entire job or the following selected items:
_____. SHU point of contact for appraisal is
_____ - phone no. _____.

SHU comments: Item #15 CTAD Repats may be permanent.

Date Sent: 8/20/2007

SHU Signature Gregory J. L. [Signature]

NWML Contact: William P. Fischer, NWML	Room number: 2100
	Phone No.: 301-837-1907

REQUEST FOR STAKEHOLDER UNIT ACTION

Job No. N1-59-07-11

Date sent: 8/6/07

Date received: 8-7-2007

Return to sender by: 8/13/07

MRH 0812/07

Route To: (CIRCLE APPROPRIATE STAKEHOLDER)
1. NWME; NWMW; <u>NWMD</u>; NWCS; NWCT; NWCTC; NWCTM; NWCTF; NWCTB; NWL; NR
Return to: William Fischer, NWML, 2100, A2

- A. This Job has also been sent to: **NWME; NWMW; NWMD; NWCS; NWCTC; NWCTM; NWCTF; NWCTB; NWL; NR; NWCT**
- B. NWML general comments on this job:
- C. NWML wishes assistance in appraising these records:

FOR STAKEHOLDER USE. Check and fill out the line that applies.

- 1. Waives informal review. ___ wants / does not want to receive completed job.
- ___ 2. Wishes to review appraisal report. ___ wants / ___ does not want to receive completed job.
- ___ 3. Wishes to participate directly in the appraisal of the entire job or the following selected items: _____ . SHU point of contact for appraisal is _____ - phone no. _____

SHU comments: _____

Date Sent: 8-17-2007 SHU Signature Madeleine Proctor

NWML Contact: William P. Fischer, NWML	Room number: 2100
	Phone No.: 301-837-1907

REQUEST FOR STAKEHOLDER UNIT ACTION

Job No. N1-59-07-11

Date sent: 8/6/07

Date received: _____

Return to sender by: 8/13/07

Route To: (CIRCLE APPROPRIATE STAKEHOLDER)
1. NWME; NWMW; NWMD; NWCS; NWCT; NWCTC ; NWCTM; NWCTF; NWCTB; NWL; NR
Return to: William Fischer, NWML, 2100, A2 ^{WPF} <u>8/10/07</u>

- A. This Job has also been sent to: ~~NWME~~; ~~NWMW~~; ~~NWMD~~; NWCS; NWCTC; NWCTM; NWCTF; NWCTB; NWL; NR; NWCT
- B. NWML general comments on this job:
- C. NWML wishes assistance in appraising these records:

FOR STAKEHOLDER USE. Check and fill out the line that applies.

1. Waives informal review. wants / ___ does not want to receive completed job.
- ___ 2. Wishes to review appraisal report. ___ wants/___ does not want to receive completed job.
- ___ 3. Wishes to participate directly in the appraisal of the entire job or the following selected items: _____ . SHU point of contact for appraisal is _____ - phone no. _____ .

SHU comments: _____

Date Sent: 8/9/07 SHU Signature: [Signature]

NWML Contact: William P. Fischer, NWML	Room number: 2100
	Phone No.: 301-837-1907

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

NI-05907-11

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

Archivist of the United States

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 _____ page(s) are not now needed 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 of the GAO Manual for Guidance of Federal Agencies:



is not required



is attached



has been requested

Signature of Agency Representative

Margaret G. Peppe

Title

Deputy Director for IPS and Agency Records Officer

Date (mm/dd/yyyy)

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

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 until superseded or no longer needed.

DispAuthNo: Pending

3. 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, control measures. Generates reports including computer security assessments, threat 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. Maintain five years or until superseded.

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: Pending

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. Maintain until superseded.

DispAuthNo: Pending

6. 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. Destroy when 5 years old.

DispAuthNo: Pending

7. Cyber Security Awareness Briefing Files

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

Disposition: Temporary. Maintain for one year or when superseded.

DispAuthNo: Pending.

8. 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 when superseded or when no longer needed.

DispAuthNo: Pending

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

Description: Records 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. Maintain for 10 years.

DispAuthNo: Pending

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. Maintain for 5 years or destroy when no longer needed.

DispAuthNo: Pending

11. 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 are maintained by vote number.

Disposition: Temporary. Maintain for 5 years.

DispAuthNo: Pending

12. 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. Maintain for 5 years or until certification is no longer needed.

DispAuthNo: Pending

13. 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. Maintain for 5 years.

DispAuthNo: Pending

14. 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. Maintain until no longer needed.

DispAuthNo: Pending

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 migrating 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: Temporary. Maintain until superseded or obsolete.

DispAuthNo: Pending

16. TASOB Quarterly Reports

Description: The file contains reports generated by TASOB providing overall analysis regarding CTAD activities including but not limited to briefing information and statistical reporting. Maintained electronically.

Disposition: Temporary. Maintain until no longer needed.

DispAuthNo: Pending

17. TASOB Reports

Description: Records created and retained on 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. Maintain until no longer needed.

DispAuthNo: Pending

18. 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. Maintain for 10 years old.

DispAuthNo: Pending

19.

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 event. System maintained by IRM.

a. (1) incident – Identified as a higher level cyber threat.

Disposition: Temporary. Destroy/delete when 5 years old.

DispAuthNo: Pending

20.

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. (2) paper – classified hardcopy (paper) incident

Disposition: Temporary. Destroy/delete when 5 years old.

DispAuthNo: Pending