REQUEST FOR RECORDS DISPOSITION AUTHORITY		JOB NUMBER N1-048-06-8	
TO: NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD COLLEGE PARK, MD 20740-6001		Date Received 8-15-2006	
FROM: (Agency or establishment) Department of the Interior		NOTIFICATION TO AGENCY	
2. MAJOR SUBDIVISION Office of the Secretary		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request, including amendments, is approved except for items that may be marked "disposition not approved or "withdrawn" in column 10.	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 Office of the Chief Information Officer			
4. NAME OF PERSON WITH WHOM TO CONFER Pamala R. Quallich	4. TELEPHONE NUMBER 202-208-3909	DATE 1/26/07	ARCHIVIST OF THE UNITED STATES Allen Weinstein

5. AGENCY INFORMATION

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 17 page(s) are not needed now for the business of this agency or will not be needed after the retention periods specified; and that written concurrence from the General Accounting Office, under the provisions of Title 8 of the GAO Manual for Guidance of Federal Agencies.

☑ is not required ☐ is attached; or ☐ has been requested.

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
August 4, 2006	Sue Ellen Silva for Pamala R. Quallich	Office of the Secretary Records Officer

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
	See Attached List of Record Descriptions and Requested Disposition Authorities.		

1/26/07
SL copies sent to Agency, NWMD, NWMW

Office of the Chief Information Officer
Cyber Security Program Files

File Description and Dispositions for File Plan Series 4300

4300 **Cyber Security Program Files**

The Office of the Chief Information Officer (OCIO) at the Department of the Interior (DOI) is responsible for providing policy, guidance, advice and oversight for IT security, while the senior official for IT systems at each bureau is responsible for the security and protection of bureau IT systems. The OCIO's Computer Security Program is further responsible for ensuring bureau and office compliance with Federal system and program IT security requirements, collaborating with the Department's enterprise architecture to ensure the implementation of sound security infrastructure for all DOI IT systems, and creating IT security policies, directives, standards, technical bulletins, guidelines, processes, and procedures for compliance with FISMA, OMB Memorandums and Circulars, GAO, and industry standards and best practices.

4301 **Cyber Security Program, Policy, Directives, Standards, Technical Bulletins Guidelines, Processes and Procedures Files**

These files contain official issuances and final versions of policies, directives, standards, technical bulletins, guidelines, and other processes and procedures. Files also include copies of official policies and directives developed by another office.

4301.a Policy/Directives Issued by Other Agencies/Bodies. Cyber Security Program policies and directives issued by other agencies/bodies.

Records are filed chronologically.
Disposition: TEMPORARY. Cut-off on the date of issue.
DELETE/DESTROY when superseded or when no longer needed for agency business, whichever is later.

4301.b Policy/Directives Developed and Issued by the OCIO. Cyber Security Program policies and directives developed and issued by the Cyber Security Division of the OCIO.

Records are filed chronologically in ACTIVE and INACTIVE folders.
Disposition: TEMPORARY. Cut-off on the date of issue.
DELETE/DESTROY fifteen (15) years after directive is superseded or revoked, or when no longer needed for agency business, whichever is later.

4301.c Technical Bulletins/Standards/Guidelines Developed and Issued by the OCIO. Technical bulletins, standards, and guidelines developed and Issued by the Cyber Security Division of the OCIO.

Records are filed chronologically in ACTIVE and INACTIVE folders.
Disposition: TEMPORARY. Cut-off on the date of issue.
DELETE/DESTROY fifteen (15) years after directive is superseded or revoked, or when no longer needed for agency business, whichever is later.

4301.d Processes/Procedures Developed by the Cyber Security Division. Processes and procedures developed by the Cyber Security Division of the OCIO.

Records are filed chronologically in ACTIVE and INACTIVE folders.
Disposition: TEMPORARY. Cut-off on the date of issue.
DELETE/DESTROY fifteen (15) years after directive is superseded or revoked, or when no longer needed for agency business, whichever is later.

4301.e Policy/Directives Issued By Bureaus/Offices. Policies and directives issued by bureaus and program offices.

Records are organized by bureau/office, and filed chronologically in bureau/office folders.
Disposition: TEMPORARY. Cut-off on the date of issue.
DELETE/DESTROY fifteen (15) years after superseded or when no longer needed for agency business, whichever is later.

4302 Cyber Security Program Policy, Directives, Standards, Guidelines, Processes and Procedures Development, Planning and Guidance Files

These files contain draft documentation from the development of the Department-wide Cyber Security policy, directives, standards, and guidelines issued by the OCIO. Also included are draft processes and procedures issued by CSD. The contents of the files include but are not limited to policy drafts, as may be issued for review and comment during the development cycle; transmittal cover sheets, which include distribution and instructions; comments and their resolution for the various draft records documenting drafts of the formal Cyber Security policy, including draft copies of applicable laws, statutes and regulations, as well as draft directives issued by other Federal agencies. The content of the files include, but are not limited to: draft copies of Cyber Security directives (e.g. draft bulletins such as the Departmental Manual Chapter 375 DM 19, "Information Technology Security Program", handbooks, IRM bulletins etc.) issued by the OCIO and draft copies of bureau/office Cyber Security directives. These files also contain Cyber Security's strategic and tactical plans. Records include, but are not limited to: analysis of new program requirements; communications, in the form of e-mail and memoranda to and from those involved in the planning process; and final and draft plans with supporting documents.

4302.a Policy/Directives Development Files. These files contain documents that strictly concern the drafting and development of policies and directives.

Records are filed chronologically.
Disposition: TEMPORARY. Cut-off the files after the policy is issued.
DELETE/DESTROY three (3) years after the file cut-off. If draft policies are not expected to be finalized, delete/destroy when the files are no longer needed for agency business.

4302.b Standards/Guidelines Development Files. These files contain documents that strictly concern the drafting and development of standards and guidelines.

Records are filed chronologically.
Disposition: TEMPORARY. Cut-off the files after the policy is issued.
DELETE/DESTROY three (3) years after the file cut-off. If draft policies are not expected to be finalized, delete/destroy when the files are no longer needed for agency business.

4302.c Processes/Procedures Development Files. These files contain documents that strictly concern the drafting and development of processes and procedures.

Records are filed chronologically.
Disposition: TEMPORARY. Cut-off the files after the policy is issued.
DELETE/DESTROY three (3) years after the file cut-off. If draft policies are not expected to be

finalized, delete/destroy when the files are no longer needed for agency business.

4302.d Program Planning Files. These files contain documents generated for periodic program planning and development.

Records are filed chronologically.
Disposition: TEMPORARY. Cut-off files on the last day of the period being planned. DELETE/DESTROY two (2) years after the file cut-off. If plans are not expected to be finalized, delete/destroy when the files are no longer needed for agency business.

4302.e Technical Advice/Guidance Files. These files contain records providing technical advice, direction, and guidance to or by bureaus and offices. The advice or guidance is often in response to a one-time question. The file contents include, but are not limited to: the advice or guidance provided, typically through the form of e-mail or memoranda, along with any supporting documents.

Records are filed chronologically.
Disposition: TEMPORARY. Cut-off files on the last day of the fiscal year. DELETE/DESTROY five (5) years after the file cut-off.

4302.f Strategic and Tactical Plans. These files contain long-term strategic and tactical plans developed by the program, and supporting documents.

Records are filed chronologically.
Disposition: TEMPORARY. Cut-off files on the last day of the fiscal year. DELETE/DESTROY five (5) years after the file cut-off.

4303 Cyber Security Program Committees/Meetings and Program Contacts Files

These files contain records regarding the OCIO's participation in meetings, both internal and external, that concern the functions of the Cyber Security Program. These include meeting minutes and correspondence via e-mail and memoranda. Also included under this series are contact lists for individuals at bureaus and program offices for communications regarding Cyber Security.

4303.a External Committee/Meeting Files (outside of DOI). These files concern committees/meetings with external agencies with whom OCIO is involved to stay aware of changing Cyber Security issues.

Disposition: TEMPORARY. Cut-off files on the last day of the committee's cycle. If there is no regular cycle, cut-off files on the last day of the fiscal year. DELETE/DESTROY five (5) years after the file cut-off.

4303.b Internal Committee/Meeting Files (within DOI). These files concern committees/meetings with bureaus and agencies inside the Department for the purpose of coordinating Cyber Security activities and gathering information.

Disposition: TEMPORARY. Cut-off files on the last day of the committee's cycle. If there is no regular cycle, cut-off files on the last day of the fiscal year. DELETE/DESTROY five (5) years after the file cut-off.

4303.c Bureau and Office Contacts Files. These files contain records that identify the bureaus' and offices' Cyber Security contacts. The contents of the files include, but are not limited to: contact lists and non-substantive communications between or among the bureau/office contacts, in the forms of e-mail, correspondence and memoranda.

Disposition: TEMPORARY.

DELETE or update information within 60 days after it has become obsolete or out of date, as appropriate.

4304 Cyber Security Program Project/Issues Files

These files contain records relating to non-routine, one-time substantive issues or projects arising from initiatives related to Cyber Security, such as CSEAT, CSIRC and US-CERT. These files also include, but are not limited to: correspondence; e-mail; memoranda; notes; project plans; milestone charts; and strategy and briefing papers.

4304.a Critical Infrastructures. These files contain project/issue files concerning the identification, prioritization, and protection of critical infrastructures in the Cyber Security Division, as outlined by the December 17, 2003 Homeland Security Presidential Directive/Hspd-7 (Critical Infrastructure Identification, Prioritization, and Protection).

Disposition: TEMPORARY. Cut-off files on the formal conclusion of the project or issue. DELETE/DESTROY five (5) years after cut-off or when no longer needed for agency business, whichever is later.

4304.b Project Plans. These files contain plans and strategic development for specific projects and issues.

Disposition: TEMPORARY. Cut-off files on the formal conclusion of the project or issue. DELETE/DESTROY five (5) years after cut-off or when no longer needed for agency business, whichever is later.

4304.c General Files. These files contain general project/issue files not related to either of the specific functions mentioned above.

Disposition: TEMPORARY. Cut-off files on the formal conclusion of the project or issue. DELETE/DESTROY five (5) years after cut-off or when no longer needed for agency business, whichever is later.

4305 Cyber Security Program System Certification & Accreditation (C&A) Files

The OCIO is responsible for maintaining certification and accreditation on DOI systems and the accompanying documentation such as system inventory, system security plans, C&A packages, contingency plans, assessments, and authorizations for the system to operate.

These files include copies of records relating to system security, including records documenting periodic audits or review and re-certification of sensitive applications, disaster and continuity plans, and risk analysis, as described in OMB Circular No. A-130.

4305.a C&A Package Documentation Files. Consists of Certification and Accreditation packages created by OCIO.

Arranged by bureau, then by system.
Disposition: DELETE/DESTROY seven (7) years after the end of each system's life-cycle or when the files are no longer needed for agency business, whichever is later.

4305.b C&A "Command Center" System (container) Files. These files contains documents regarding the C&A Command Center System, for the coordination and management of C&A data.

4305.b(1) Planning and Development. These files contain records relating to the initial planning and development of the system as well as records relating to its ongoing modification

and enhancement. They include but are not limited to: records relating to system authorization; documents soliciting and providing input on functional requirements; documents detailing technical specifications; plans, timetables, and milestone charts for system development; screen design mock-ups; records relating to system installation and testing; and system acceptance documents.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of the system's (Command Center's) life-cycle if all other active data has been migrated to any replacement information management system or when the files are no longer needed for agency business, whichever is later.

4305.b(2) Management and maintenance. These files contain records relating to the routine management of the system. They also contain records relating to the day-to-day maintenance of the system created or received by the system's maintenance provider. Management documents include, but are not limited to: administrative documents (documents relating to system costs and funding) and system-function documents (system Business Rules and guidelines, Rules of Behavior, etc.). Maintenance documents include, but are not limited to: electronic and hard-copy printouts created to monitor system usage (log-in files, password files, audit trail files, and system usage files), identify and correct system problems, back-up system data, and perform any other functions associated with routine and regular system maintenance and support.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of the system's (Command Center's) life-cycle if all other active data has been migrated to any replacement information management system or when the files are no longer needed for agency business, whichever is later.

4305.b(3) Input files. These files contain all C&A data entered into the system.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of the system's (Command Center's) life-cycle if all other active data has been migrated to any replacement information management system or when the files are no longer needed for agency business, whichever is later.

4305.b(4) Master data files. These files contain the master copy of data held by the C&A Command Center for the maintenance and administration of C&A functions.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of the system's (Command Center's) life-cycle if all other active data has been migrated to any replacement information management system or when the files are no longer needed for agency business, whichever is later.

4305.b(5) Security files. These files include all records relating to system security, risk analysis, and disaster and continuity planning, as described in OMB Circular No. A-130. These include, but are not limited to the following: System Security Plan, Asset Valuation*, the PIA (Privacy Impact Assessment)*, Contingency Plan, Self Assessment Checklist (NIST 800-26), Limited Technical Vulnerability Assessment, Configuration Management Plan, Risk Assessment Report, Security Testing and Evaluation Report, Certification Statement*, and accreditation Statement*. The record copy of these documents is maintained in the office of the system's Security Officer.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of the system's (Command Center's) life-cycle if all other active data has been migrated to any replacement information management system or when the files are no longer needed for agency business, whichever is later.

4305.b(6) Output (reports) files. System outputs consist of printable or exportable (electronic) reports summarizing C&A data maintained in the database sorted by a variety of categories.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of the system's (Command Center's) life-cycle if all other active data has been migrated to any replacement information management system or when the files are no longer needed for agency business, whichever is later.

4305.b(7) Documentation files. These files contain all records needed to interpret (read and understand) the data in the system. They include, but are not limited to: the system's program code and code translation tables (codebooks); data element definitions and dictionary; table descriptions; file specifications; and record layout. These records pertaining to the technical description of the electronic system are maintained in the office of the system's maintenance provider.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of the system's (Command Center's) life-cycle if all other active data has been migrated to any replacement information management system or when the files are no longer needed for agency business, whichever is later.

4305.b(8) User Manual and Training files. These files contain records created to train or assist authorized systems users in using the system, and records relating to the administration of training in the use of the system provided to system users. They include, but are not limited to: printed and electronic user guides, electronic "Help Screen" instructions, Power Point presentations, handouts prepared for system demonstrations and user training, announcements of and schedules for user training sessions, sign-in sheets documenting users trained, and other related records. The record copy of these files is maintained in the office of the system's maintenance provider.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of the system's (Command Center's) life-cycle if all other active data has been migrated to any replacement information management system or when the files are no longer needed for agency business, whichever is later.

4305.c C&A, General Files. These files include documents created in the process of generating official C&A documents, such as C&A packages and Command Center System Files.

4305.c(1) Presentations, Graphs, Charts. These files contain presentations, graphs, charts, and other visual aids used to display C&A information.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of each system's life-cycle or when the files are no longer needed for agency business, whichever is later.

4305.c(2) Memos, emails, faxes. These files contain administrative correspondence, including but not limited to the forms of memos, emails, and faxes.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of each system's life-cycle or when the files are no longer needed for agency business, whichever is later.

4305.c(3) Meeting Notes, Meeting Agenda, C&A Summary Reports. These files contain meetings notes, agendas, and summary reports not included in official reports and meeting

minutes.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of each system's life-cycle or when the files are no longer needed for agency business, whichever is later.

4305.c(4) Methodology, Checklists, Frameworks, C&A Process. These files contain notes and documents on methodology, routine checklists, frameworks, and other miscellaneous files accumulated in planning other documents.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of each system's life-cycle or when the files are no longer needed for agency business, whichever is later.

4305.c(5) Systems Inventory. These files include routine systems inventories for the maintenance and management of the C&A system.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of each system's life-cycle or when the files are no longer needed for agency business, whichever is later.

4305.c(6) Privacy Impact Assessments. These files contain Privacy Impact Assessments and documents related to their creation.

Disposition: TEMPORARY.
DELETE/DESTROY seven (7) years after the end of each system's life-cycle or when the files are no longer needed for agency business, whichever is later.

4306 Cyber Security Program Plan of Action & Milestones (POA&M)

The CSD covers all activities that contribute to the delivery of POA&M reports to OMB and provides support to Bureau IT Security Managers (BITSM)s to assist in their effort to manage and remediate weaknesses and vulnerabilities to IT systems. CSD provides a consolidated quarterly package to the CIO for submission to OMB. The files also include exhibit 300 reviews and supporting bureau and office data files.

4306.a Bureau/Office Data Files. These files include data and information from bureaus and program offices supporting POA&M reports.

Arranged by fiscal year, OMB reporting quarter, bureau, then by system.

Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

4306.b Quarterly OMB POA&M Package. These files contain supporting information for the Cyber Security Program quarterly POA&M report.

Arranged by fiscal year then OMB reporting quarter.

Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

4306.c Exhibit 300s. These files contain reviews for compliance with Exhibit 300 (Capital Asset Plan and Business Case Summary) of OMB Circular A-11, PART 7-PLANNING, BUDGETING, ACQUISITION, AND MANAGEMENT OF CAPITAL ASSETS.

Arranged by fiscal year then OMB reporting quarter.

Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

4307 Cyber Security Program Enterprise Security Architecture Files

The Cyber Security Division (CSD) Enterprise Security Architecture (ESA) aligns security with DOI's business mission and IT mission priorities. ESA validates its recommendations according to these parameters and ensures that the recommendations and guidance are consistent with IT security policies and Secure Technical Implementation Guidelines (STIG). The ESA is responsible for maintaining enterprise architecture files such as waiver requests, e-authentication files, and STIGs.

4307.a Waiver Requests Files. Files include waiver requests to ESA and all supporting documentation.

Disposition: TEMPORARY. Cut-off on the date of issue.
DELETE/DESTROY five (5) years after superseded, or when no longer needed for agency business, whichever is later.

4307.b E-Authentication Files. Files include electronic and paper copies of e-authentication files for security maintenance and monitoring.

Disposition: TEMPORARY. Cut-off on the date of issue.
DELETE/DESTROY five (5) years after superseded, or when no longer needed for agency business, whichever is later.

4307.c Secure Technical Implementation Guidelines (STIG). Files contain documents generated by ESA for compliance with STIG and any documents relating to the formulation or analysis of those and related guidelines.

Disposition: TEMPORARY. Cut-off on the date of issue.
DELETE/DESTROY five (5) years after superseded, or when no longer needed for agency business, whichever is later.

4307.d Enterprise Security Architecture Standards. Files contain correspondence, guidance, and other files pertaining to ESA Standards and requirements, including final documents for release.

Disposition: TEMPORARY. Cut-off on the date of issue.
DELETE/DESTROY five (5) years after superseded, or when no longer needed for agency business, whichever is later.

4308 Cyber Security Program Computer Incident Coordination Center Files

The OCIO is responsible for maintaining incident coordination center files such as incident monitoring and reporting documentation.

Electronic files and hard-copy printouts created to monitor system usage, including, but not limited to log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system use.

4308.a Incident Files. Files contain records of incidents and incident management within the Cyber Security Program.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.a(1) Weekly. Files that are produced on a weekly basis.

4308.a(1.1) Teleconference minutes. These files contain minutes of teleconferences specifically concerning incident reports, analyses, and management.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for Administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.a(1.2) Vulnerability Notices and Alerts. These files contain vulnerability notices and alerts concerning actual or suspected incidents.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for Administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.a(1.3) Incident Reports. These files contain weekly incident reports.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for Administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.a(1.4) Summary Reports. These files contain weekly summary reports.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for Administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.a(2) Monthly. Files that are produced on a monthly basis.

4308.a(2.1) Vulnerability Notices and Alerts. These files contain vulnerability notices and alerts concerning actual or suspected incidents.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for Administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.a(2.2) Incident Reports. These files contain monthly incident reports.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for Administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.a(2.3) Summary Reports. These files contain monthly summary reports.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for Administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.a(3) Annually. Files that are produced annually.

4308.a(3.1) Reports. These files contain reports on incidents and incident trends produced from weekly and monthly summary and incident reports.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for Administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.a(3.2) Analysis. These files contain annual analyses of system vulnerability and proposed prevention for future incidents.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for Administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.b Incident Tracking System Files. Files contain documents relating to the Incident tracking System, which tracks and monitors incidents and incident trends.

4308.b(1) Management and Maintenance. These files contain records relating to the routine management of the system. They also contained records relating to the day-to-day maintenance of the system created or received by the system's maintenance provider. Management documents include, but are not limited to: administrative documents (documents relating to system costs and funding) and system-function documents (system Business Rules and guidelines, Rules of Behavior, etc.). Maintenance documents include, but are not limited to: electronic and hard-copy printouts created to monitor system usage (log-in files, password files, audit trail files, and system usage files), identify and correct system problems, back-up system data, and perform any other functions associated with routine and regular system maintenance and support.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.b(2) Input files. Data for each incident entered directly into the system.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.b(3) Master data files. These files contain the master copy of data used and maintained by the Incident Tracking System.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.b(4) Security files. These files include all records relating to system security, risk analysis, and disaster and continuity planning, as described in OMB Circular No. A-130. These include, but are not limited to the following: System Security Plan, Asset Valuation*, the PIA (Privacy Impact Assessment)*, Contingency Plan, Self Assessment Checklist (NIST 800-26), Limited Technical Vulnerability Assessment, Configuration Management Plan, Risk Assessment Report, Security Testing and Evaluation Report, Certification Statement*, and accreditation Statement*. The record copy of these documents is maintained in the office of the system's Security Officer

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.b(5) Output (reports) files. System outputs consist of printable or exportable (electronic) reports summarizing incident data maintained in the database sorted by a variety of categories.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.b(6) Documentation files. These files contain all records needed to interpret (read and understand) the data in the system. They include, but are not limited to: the system's program code and code translation tables (codebooks); data element definitions and dictionary; table descriptions; file specifications; and record layout. These records pertaining to the technical description of the electronic system are maintained in the office of the system's maintenance provider in the NBC.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.b(7) User Manual and Training files. These files contain records created to train or assist authorized systems users in using the system, and records relating to the administration of training in the use of the system provided to system users. They include, but are not limited to: printed and electronic user guides, electronic "Help Screen" instructions, Power Point presentations, handouts prepared for system demonstrations and user training, announcements of and schedules for user training sessions, sign-in sheets documenting users trained, and other related records. The record copy of these files is maintained in the office of the system's maintenance provider in the NBC.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4308.c Incident Files – General. These files contain general records generated as supporting documents and working files for the creation of incident reports, summaries, and other official documents; included are correspondence via email or memoranda, notes, charts and graphs, and other miscellaneous documents.

Disposition: TEMPORARY. Cut-off when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes.
DELETE/DESTROY three (3) years after all necessary follow-up actions have been completed.

4309 Cyber Security Program Reports Files

The primary objective of the CSD program reports is to ensure bureau and office compliance with Federal System and Program IT Security requirements and prepare them for external audits through consistent assessment and feedback. Compliance reporting assures regulatory agencies (e.g., Congress, OMB, GAO) that the Agency continually maintains security on their IT systems. CSD is responsible for maintaining program reports files such as monthly Congressional scorecards, annual Federal Information Security Management Act (FISMA) reports, Internal Control Reviews (ICR), OIG test, evaluation, and compliance reports, and annual assurance statements.

4309.a Regulatory Control reports. These files contain documents concerning the reports issued and received regarding bureau and office compliance with regulatory controls, limitations, standards, and guidelines. Regulatory Reports include scorecards, checklists and presentations, and other reports concerning compliance with IT and Cyber Security requirements.

Arrange by fiscal year, by bureau.

4309.a(1) Congressional scorecards. These files contain Congressional scorecards to evaluate bureau and program office compliance with federal standards.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4309.a(2) Annual FISMA reports. These files contain annual reports in compliance with FISMA and documents pertaining to their creation.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4309.a(3) Monthly Interior IT Scorecards. These files contain scorecards generated for bureau and office compliance with Interior IT standards.

4309.a(3.1) CIO Scorecard and Checklist. These files contain scorecards and checklists generated by CIO in support of Monthly Interior IT Scorecards.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4309.a(3.2) Scorecard Presentations. These files contain documents relating to the presentation of Monthly Interior IT Scorecards.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4309.a(4) Internal Control Reviews (ICR). These files contain internal control reviews to verify compliance with established regulations and requirements.

Arranged by fiscal year, by bureau, by system.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4309.a(5) Performance Accountability Reports (PAR) and Assurance Statements. These files contain performance accountability reports and assurance statements to confirm compliance with established standards and requirements.

Arrange by fiscal year, by bureau.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4309.b Internal Compliance reports. These files contain documents relating to Internal Compliance reports, including program review assessments, vulnerability scanning, audit support, compliance inspections, and performance reporting.

Arrange by fiscal year, by bureau, by system.

4309.b(1) Program Review Assessments. These files contain program review assessments for assurance of bureau and office compliance with established rules and regulations.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4309.b(2) Vulnerability Scanning. These files contain documents pertaining to vulnerability scanning and other files monitoring potential security weaknesses in bureau and office cyber security.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4309.b(3) Audit Support. These files contain documents preparing bureaus and offices for audits, including feedback, assessments, and any resulting copies of the audit or previous audits used for information and reference or other supporting documentation.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4309.b(4) Compliance Inspection. These files concern compliance inspections of bureau and office cyber security functions or systems and all supporting documentation created for such inspections.

> **4309.b(4.1)** FISMA – General. These files contain general information for reports in compliance with the FISMA Implementation Plan.
>
> Reports received:
> Disposition: TEMPORARY. Cut-off on the date of report.
> DELETE/DESTROY when no longer needed for agency business.
>
> Reports issued and supporting documentation:
> Disposition: TEMPORARY. Cut-off on the date the report is issued.
> DELETE/DESTROY five (5) years after cut-off.
>
> **4309.b(4.2)** Office of Inspector General (OIG) FISMA Data Calls. These files contain data collecting in response to OIG data calls and related information.
>
> Reports received:
> Disposition: TEMPORARY. Cut-off on the date of report.
> DELETE/DESTROY when no longer needed for agency business.
>
> Reports issued and supporting documentation:
> Disposition: TEMPORARY. Cut-off on the date the report is issued.
> DELETE/DESTROY five (5) years after cut-off.

4309.b(5) Performance Reporting. These files contain internal performance reporting relating to bureau and office compliance with established regulations and requirements.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.

DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4309.c Policy, Management and Budget reports. These files contain reports for policy, management, and budget. Files also include all related material for the formation of these reports, including, but not limited to: correspondence in the form of email or memoranda, notes, and other working materials.

Arrange by fiscal year, by bureau.

Reports received:
Disposition: TEMPORARY. Cut-off on the date of report.
DELETE/DESTROY when no longer needed for agency business.

Reports issued and supporting documentation:
Disposition: TEMPORARY. Cut-off on the date the report is issued.
DELETE/DESTROY five (5) years after cut-off.

4310 Cyber Security Program Court Files (Trust)

The OCIO is responsible for maintaining documentation of pending court cases relevant to the Cyber Security Division. These files include court orders, court actions, and reports to the court. These files contain copies of court or litigation-related documents affecting the security posture of the Department.

These files are classified as Indian Fiduciary Trust (IFT) records.

4310.a Court Order Files (Trust). These files contain CSD copies of court orders that directly impact Cyber Security policy and procedures. These files also include site visits to ensure compliance with court orders.

Arranged by Bureau.

Disposition: PERMANENT. Cut-off files upon the expiration of an individual court order or upon closure of the related case or any related appeals.
RETIRE to Federal Records Center six (6) years after the cut-off of final court action or when no longer needed for agency business. Subsequent legal transfer of the records to the National Archives of the United States will be as jointly agreed to between the United States Department of Interior and the National Archives and Records Administration.

4310.b Court Action Files (Trust). These files CSD copies of court actions affecting Cyber Security policy and procedures.

Arranged by Bureau.

Disposition: PERMANENT. Cut-off files upon the expiration of an individual court order or upon closure of the related case or any related appeals.
RETIRE to Federal Records Center six (6) years after the cut-off of final court action or when no longer needed for agency business. Subsequent legal transfer of the records to the National Archives of the United States will be as jointly agreed to between the United States Department of Interior and the National Archives and Records Administration.

4310.c Reports To The Court (Trust). These files contain CSD reports to the court on cyber security progress and development, as required by court orders and actions. These files also include requests to reconnect and other associated requests.

Arranged by Bureau.

Disposition: PERMANENT. Cut-off files upon the expiration of an individual court order or upon closure of the related case or any related appeals.
RETIRE to Federal Records Center six (6) years after the cut-off of final court action or when no longer needed for agency business. Subsequent legal transfer of the records to the National Archives of the United States will be as jointly agreed to between the United States Department of Interior and the National Archives and Records Administration.

4310.d Input to Workings of the Court (Trust). These files contain working copies and supporting documents used for the generation of quarterly reports to the court. Included are reports from bureaus and offices to be included in the quarterly report.

Arranged sequentially according to court assigned quarters.

4310.d(1) CSD Working Files and input to the Quarterly Report. These files contain documents generated for the quarterly report and for any data contributing to the quarterly report.

Disposition: PERMANENT. Cut-off files upon the expiration of an individual court order or upon closure of the related case or any related appeals.
RETIRE to Federal Records Center six (6) years after the cut-off of final court action or when no longer needed for agency business. Subsequent legal transfer of the records to the National Archives of the United States will be as jointly agreed to between the United States Department of Interior and the National Archives and Records Administration.

4310.d(2) Bureaus/Offices Quarterly Report. These files contain quarterly reports from bureaus and program offices that are to be referenced and included in quarterly reports to the court.

Disposition: PERMANENT. Cut-off files upon the expiration of an individual court order or upon closure of the related case or any related appeals.
RETIRE to Federal Records Center six (6) years after the cut-off of final court action or when no longer needed for agency business. Subsequent legal transfer of the records to the National Archives of the United States will be as jointly agreed to between the United States Department of Interior and the National Archives and Records Administration.

4311 Cyber Security Program DOI Training Files

The OCIO is responsible for maintaining files relating to the training provided by the OCIO on Cyber Security program requirements. These files include training administration, course development, and course product files.

4311.a DOI Training Administration Files. These records include information regarding the availability, planning, scheduling, logistics, and attendance of training. Records include, but are not limited to: memoranda, e-mails, correspondence, flyers or announcements, sign-in sheets, reports, and related files.

Disposition: TEMPORARY. Cut-off files on the last day of the fiscal year.
DELETE/DESTROY five (5) years after the file cut-off.

4311.b DOI Training Course Development Files. These files contain records of the development of training products used for training or educational purposes. The contents of the

files include, but are not limited to: draft content and communications in the forms of e-mail or memoranda related to course.

Disposition: TEMPORARY. Cut-off files once the course content is finalized.
DELETE/DESTROY after file cut-off or when no longer needed for agency business, whichever is later. If training course development files are not expected to be finalized, delete/destroy when the files are no longer needed for agency business.

4311.c DOI Training Course Product Files. These files contain the actual products of any formal or informal Cyber Security training, including educational outreach communications. Products include, but are not limited to: instructions; tips; pamphlets; lesson plans; agendas and outlines; Power Point training slides; supplemental handout materials; and educational information on the Cyber Security Program.

Disposition: TEMPORARY. Cut-off files on the date the product is substantively superseded or becomes obsolete.
DELETE/DESTROY one (1) year after the file cut-off or when no longer needed for agency business, whichever is sooner.

4312 Cyber Security Program Website Files

The OCIO is responsible for maintaining files pertaining to electronic links to documents relating to Cyber Security as posted on the Department's website at www.doi.gov. The files contain information about the Department's IT security program.

Disposition: TEMPORARY.
DELETE/or update information within 60 days after it has become obsolete or out of date, as appropriate.

4313 Cyber Security Program Electronic Mail and Word Processing System Files

Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by this schedule, and electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

4313.a CD's. Files stored on CDs.

Disposition: TEMPORARY.
DELETE/DESTROY within 180 days after the record keeping copy has been produced, or when dissemination, revision or updating is completed, as appropriate.

4313.b Diskettes. Files stored on diskette.

Disposition: TEMPORARY.
DELETE/DESTROY within 180 days after the record keeping copy has been produced, or when dissemination, revision or updating is completed, as appropriate.

GRS 20
#13+14

SF 115 Supplementary Cover Sheet

Summary:

This action establishes a new Office of the Secretary series entitled: "Cyber Security Program Files."

Reason for submission:

(1) This action provides for the disposition of records that document the Department's Cyber Security Program. Responsibility for this program is vested in the Cyber Security Division of the Office of the Chief Information Officer, within the Office of the Secretary of the Department of the Interior.

(2) This action also *incorporates the series into the numbering pattern of the Office of the Secretary's new records schedule*. See attachment.

Crosswalk

New OS Records Schedule		Old OS Records Schedule	
1000	Administration, Planning and Performance	A.	Office Administration (100)
1200	Strategic Planning & Performance Assessment Files	B.	Management and Planning (200)
1300	Management Improvement Files		
2000	Budget and Financial Management	C.	Budget and Finance (300)
3000	Human Resources Management	D.	Personnel (400)
4000	Information Management	I.	Public Relations (900)
4300	Cyber Security Program Files	Not covered by old schedule.	
5000	Procurement and Property Management	E.	Procurement and Property (500)
6000	Law Enforcement and Security	F.	Security and Law Enforcement (600)
7000	Legal and Legislative	H.	Legal and Legislative (800)
8000	Audit and Investigation	G.	Audit and Investigation (700)
9000	Office of the Secretary Programs	J.	Research and Development (1000)
		K.	Program/Projects (1100)