REQUEST FOR RECORDS DISPOSITION AUTHORITY

(See Instructions on reverse)

TO: NATIONAL ARCHIVES and RECORDS ADMINISTRATION (NIR)
WASHINGTON, DC 20408

LEAVE BLANK (NARA use only)
JOB NUMBER: N1-434-05-2
DATE RECEIVED: 4-7-2005

1. FROM (Agency or establishment)
U. S. Department of Energy

2. MAJOR SUBDIVISION
Office of Counterintelligence (OCI)

3. MINOR SUBDIVISION
N/A

4. NAME OF PERSON WITH WHOM TO CONFER	5. TELEPHONE
Anthony Z. S. Bailey, Chief Information Officer for OCI	202-586-1721

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request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.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
8/1/07	

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; or ☐ has been requested.

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
03/12/2005	Sharon A. Evelin	Records Officer, U. S. Department of Energy

7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
	Series 1: Program Administrative Policy and Procedures. DOE Office of Counterintelligence/Office of Nuclear Counterintelligence Administrative Correspondence, Program Policy&Procedures; Admin Management/Procedures; historical CI Investigation Procedures and Foreign Intelligence Policy/Procedures Series 2: Public Relations and Liaisons w/Agencies. Includes records of liaisons with external and internal agencies in intelligence, law enforcement, security, Congressional/Presidential; DOE laboratories, counterintelligence field elements and NNSA to facilitate sharing intelligence information (reports, MOU, MOA). Series 3: Case Files and Program Specific Files. Investigative case files and program specific files used for counterintelligence including ongoing and completed case files of subject material or projects relating to each program's mission. Series 4: Reporting and Distribution of CI Products. Final documentation of intelligence products in the form of Periodic Reports, Trending Analyses, publications, of both internal and external liaisons such as IIR, GAO, Cox Report, Espionage Open Source Articles, Collection and Threat Publications. Series 5: Counterintelligence Enterprise Architecture (CI-EA) database application and Counterintelligence Analytical Research Data System (CARDS). Includes modules for the programs of Investigations, Analysis, Evaluations, Polygraph and Inspections, used as a network database tool to process classified. All 5 SERIES ABOVE CLASSIFIED UP TO SECRET		

AH 8/6/07 Copies sent to Agency NWMD, NWME, NWMWA, NR

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 Energy

2. Major Subdivision
Office of Counterintelligence

3. Minor Subdivision
N/A

4. Name of Person with whom to confer
Anthony Z.S. Bailey,CIO/OCI

5. Telephone (include area code)
202-586-1721

Leave Blank (NARA Use Only)

Job Number

Date Received

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:

[X] is not required [ ] is attached [ ] has been requested

Signature of Agency Representative	Title	Date (mm/dd/yyyy)
	Records Officer, U.S.Department of Energy	10/25/2005

7. Item Number	8. Description of Item and Proposed Disposition	9. GRS or Superseded Job Citation	10. Action taken (NARA Use Only)
	This schedule applies to records regardless of physical format or media. See Attached Office of Counterintelligence Records Schedule, Items 1-19.		

OFFICE OF COUNTERINTELLIGENCE and OFFICE OF DEFENSE NUCLEAR COUNTERINTELLIGENCE

RECORDS SCHEDULE COUNTERINTELLIGENCE RECORDS

Purpose

This schedule identifies the records generated by the Department of Energy's Counterintelligence Program Office. The Office of Counterintelligence records consist of the Department's Headquarter Program Office, its Operations Offices, National Laboratories, Area Offices, Site, Regional and Project Offices. Additionally, the Defense Nuclear Counterintelligence Program includes records of the National Nuclear Security Administration, its Operations Offices and National Laboratories. The appropriate retention and disposition of counterintelligence records are critical to:

> Controlling, obtaining and maintaining the documentation necessary to maintain an efficient stockpile of intelligence and counterintelligence information is utmost in the endeavor to create, retrieve, search and share with entities within the Department of Energy, FBI, CIA, NACIC and other intelligence community agencies.

The mission of the Office of Counterintelligence is:

> Conduct CI activities to protect DOE/NNSA classified and sensitive programs and information, personnel, and assets from foreign intelligence collection and international terrorist activities; and to detect and deter trusted insiders who would engage in activities on behalf of a foreign intelligence service or foreign terrorist entity.

After review, records for selected projects representing technological advancements of historical significance will be offered to the National Archives and Records Administration (NARA). National security issues shall be addressed before the transfer of the selected records occurs. All information will be transferred by the offering agency as a complete unit for each selected project.

The four record series are identified in this schedule as follows:

Series 1: Program Administrative Policy and Procedures

DOE Office of Counterintelligence/Office of Nuclear Counterintelligence Administrative Correspondence including Program Policy and Procedures; Administrative Management and Procedures; Historical CI Investigation Procedures and Foreign Intelligence Administration Policy and Procedures.

Series 2: Intelligence Community Liaisons

Includes records of liaisons with external and internal agencies in intelligence, law enforcement, security, governmental; DOE laboratories, counterintelligence field elements and NNSA to facilitate sharing intelligence information. The records can be reports, MOA, MOU, administrative correspondence intelligence information, presentations.

Series 3: Case Files and Program Specific Files

Investigative case files and program specific files used for counterintelligence including ongoing and completed case files of subject material or projects relating to each program's mission.

Series 4: Electronic Network System Processing

Electronic database modules used by OCI programs such as Operations and Investigation, Analysis, Evaluations, Inspections and Polygraph Programs for classified processing.

The records within these four series are media neutral and can be classified up to Top Secret.

Series 1: Program Administrative Policy and Procedure

Series Detailed Description: DOE Office of Counterintelligence/Office of Nuclear Counterintelligence Administrative Correspondence including Program Policy and Procedures; Administrative Management and Procedures; Historical CI Investigation Procedures and Foreign Intelligence Administration Policy and Procedures.

Item 1: Counterintelligence Correspondence, DOE Policy, Management and Procedures, Administrative Management, Programs Administrative Records; Historical CI Investigation Procedures and Foreign Intelligence.

Disposition: Transfer to the National Archives when record is 25 years old after declassification review. When records to be transferred are electronic, DOE and NARA will determine, at the time of transfer, the media and format of the records to be transferred, in accordance with the standards for permanent electronic records contained in 36 CFR 1228.270 or standards applicable at that time. Also, when records to be transferred are electronic, physical custody may be transferred to the National Archives before they are 25 years old, at the mutual agreement of DOE and NARA. **PERMANENT**

Item 2: Documentation for processing and presentation of credentials and mentoring program to be used in counterintelligence investigation or inspection requirements, including to and from post assignments, appointments, letters of correspondence, and issuance and termination of credential.

Disposition: Cut off upon termination of requirement for use of or termination in position requiring credential. Destroy 2 years after cutoff. **TEMPORARY**

Series 2: Intelligence Community Liaisons

Series Detailed Description: Includes records of liaisons with external and internal agencies in intelligence, law enforcement, security, governmental; DOE laboratories, counterintelligence field elements and NNSA to facilitate sharing intelligence information. The records can be reports, MOA, MOU, administrative correspondence intelligence information, presentations.

Item 3: Presidential Reports, external guidance, commissions and resultant action item resolutions, periodic conferences, meetings, site reviews, and requests from NNSA, field sites and DOE laboratories.

Disposition: Destroy 2 years after completion of all action item resolutions. **TEMPORARY**

Item 4: Intelligence Assessments. Final version and related source copy of each periodic report, intelligence threat assessment, intelligence memorandum; Technical Intelligence Notes (TINS) and Special Reports; data in the Secure Intelligence Analysis Production System (SINAPS), or other products produced by DOE or produced for another organization for which DOE/OCI served as coordinator or chairperson.

Disposition: Transfer to the National Archives when record is 25 years old after declassification review. When records to be transferred are electronic, DOE and NARA will determine, at the time of transfer, the media and format of the records to be transferred, in accordance with the standards for permanent electronic records contained in 36 CFR 1228.270 or standards applicable at that time. Also, when records to be transferred are electronic, physical custody may be transferred to the National Archives before they are 25 years old, at the mutual agreement of DOE and NARA. **PERMANENT**

Item 5: Liaison and Outreach to Congress, external and internal agencies through councils, working groups, task force or sub work groups.

Disposition: Destroy when record is 15 years old. **TEMPORARY**

OFFICIAL USE ONLY

Series 3: Case Files and Program Specific Files

Series Detailed Description: Investigative case files and program specific files used for counterintelligence including ongoing and completed case files of subject material or projects relating to each program's mission.

Item 6: Working Files including reports, notes, drafts, working papers and other records used, created or circulated by OCI staff in developing an intelligence threat assessment, the final case file report, intelligence publication or other product resulting from the gathered working information.

Collection of information for use as potential counterintelligence or counterterrorism value, and contact reports. Also included are the collection, publication and distribution of intelligence data including procedures, working documentation, distribution lists, intelligence threat assessment, intelligence memoranda, e-mail and reports.

Documents, submissions, substantive drafts, comments, or other records which **ARE ESSENTIAL** to the understanding of DOE/OCI's formulation and execution of policies, decisions, or programs and Requests for Information Management. (See item #10 for non-essential).

Disposition: Destroy when 15 years old. **TEMPORARY**

Item 7: Program Products including Specific Country Information, Foreign Entities, Sensitive Technologies List, Sanctioned Entities, List CI Notes, Foreign Intelligence Threat Summaries (FITS), comprehensive assessments, counterterrorism reporting/analysis and special assessments.

Disposition: Use Item 4 Disposition. **PERMANENT**

Item 8: Correspondence on High Risk Access and Completed Access Evaluations. Includes points of contact lists, communications with high-risk program managers and security administrators, challenges to polygraph evaluations, notifications, videotapes of polygraph tests; electronic databases and spreadsheets; Issue cases, Code of Conduct letters; and access recommendations. Also included are completed Financial Analysis case files, database records review, and reports from commercial databases (Choicepoint, Autotrac, Equifax).

Disposition: Destroy when 10 years old, on when two five-year polygraph exams have been completed. **TEMPORARY**

OFFICIAL USE ONLY

Item 9: Investigative Case Files Open and Closed. Case files include inserts, correspondence both e-mail and written, threat assessment, foreign intelligence sources and indices check. Also included are special projects or case files on HEU or Nuclear project program that are not electronically included in CI-EA, but identified as part of a case.

Disposition: Destroy **paper** case files when 75 years old, unless needed longer for current business needs. **TEMPORARY**

NOTE: **Non-electronic inserts cannot be orphaned from a case in CI-AIMS.**

Item 10: Intelligence Assessments. Working Files includes reports, notes, drafts, working papers and other records used, created or circulated by OCI staff in developing an intelligence threat assessment, final report, publication or other product. These submissions, notes, drafts, comments or other records are **NOT ESSENTIAL** to the understanding of DOE/OCI's formulation of policy. (See item #6 for essential).

Disposition: Destroy when record is 5 years old. **TEMPORARY**

Item 11: OCI Inspection documentation including working papers, logistics for site inspections (travel arrangements, equipment shipping, package wrapping), and scheduling of inspection team and inspection site.

Disposition: Destroy when record is 2 years old. **TEMPORARY**

Item 12: OCI/ODNCI Final Inspection Reports on Programs and Field Sites that include final report, findings/recommendations, responses to findings and closeout.

Disposition: Destroy when record is 10 years old. **TEMPORARY**

Item 13: Counterintelligence/Counterterrorism Working Groups and resultant documentation, intelligence publications or policy to facilitate adhering to the OCI/ODNCI mission. This includes The CT Council, CT/WMD Working Group, Combating Terrorism Intelligence WG, Foreign Terrorism Tracking Task Force (FTTF) and various working or sub-working groups in the intelligence arena.

Disposition: Destroy when record is 2 years old. **TEMPORARY**

OFFICIAL USE ONLY

Item 14: Polygraph Tests, Selection of test types, Periodic Reports, Trending Analyses, Spreadsheets and database information from CI-ACTS, CI-AIMS, CI-POLY, Scheduling Roster and logistics used to perform scheduling. Also includes lists of new and incumbent staff, contact information and scheduling calendars that facilitate processing polygraph testing.

Disposition: Destroy when record is 25 years old. **TEMPORARY**

Item 15: Final Polygraph Test Results and associated completed forms or documentation required to request and complete a polygraph test.

Disposition: Destroy when record is 25 years old. **TEMPORARY**

Item 16: Counterintelligence Course Outlines, Logistics for each course, Program Schedule of Classes (by title, by program), SCIO Conference Agenda and logistics, meeting minutes, member database for CI Awareness, attendee lists, Certificates of Completion all related to OCI/ODNCI training.

Disposition: Destroy when the record is 15 years old. **TEMPORARY**

Item 17: CARDS Database Training for data input and documentation retrieval. The training documentation includes submitted requests, scheduling logistics, completion test, certificates, comments and suggestions.

Disposition: Destroy OCI copy when 7 years old. (Note: Record to be sent to OPF when 5 years old.) **TEMPORARY**

Item 18: Documentation of polygraph test results and evaluation of Quality Control and testing processes used to facilitate performance evaluations and ensure polygraph criteria are met and adhered to as a means of evaluating staff's performance when administering polygraph testing.

Disposition: Destroy OCI copy when 25 years old. (Note: Record to be sent to OPF in blocks of 5 year-old-groups.) **TEMPORARY**

Series 4: Electronic Network System Processing

Series Detailed Description: Electronic database modules used by OCI programs such as Operations and Investigation, Analysis, Evaluations, Polygraph, and Inspections Programs for classified processing.

Item 19: Data that is stored in relational databases where the resultant output is in the form of documents or reports from electronic databases such as CARDS, *web*CARDS, CI-AIMS, CI-POLY, CI-EVAL, IIRs, and etcetera. Also included are database modules for processing, maintaining and updating access evaluations, financial analyses and investigations.

Hosts Briefing and Debriefing of Foreign Visitors and Assignments, and etc. These two items include initial CI briefing and documentation into CARDS.

Disposition: Destroy record when 75 years old, or when system and data are superseded or replaced, or when mission requirements dictate system obsolescence, whichever is later. **TEMPORARY**

Series 1: Program Administrative Policy and Procedure

Series Detailed Description: DOE Office of Counterintelligence/Office of Nuclear Counterintelligence Administrative Correspondence including Program Policy and Procedures; Administrative Management and Procedures; Historical CI Investigation Procedures and Foreign Intelligence Administration Policy and Procedures.

Item 1: Counterintelligence Correspondence, DOE Policy, Management and Procedures, Administrative Management, Programs Administrative Records; Historical CI Investigation Procedures and Foreign Intelligence.

Disposition: Transfer to the National Archives when record is 25 years old after declassification review. When records to be transferred are electronic, DOE and NARA will determine, at the time of transfer, the media and format of the records to be transferred, in accordance with the standards for permanent electronic records contained in 36 CFR 1228.270 or standards applicable at that time. Also, when records to be transferred are electronic, physical custody may be transferred to the National Archives before they are 25 years old, at the mutual agreement of DOE and NARA. **PERMANENT**

Item 2: Documentation for processing and presentation of credentials and mentoring program to be used in counterintelligence investigation or inspection requirements, including to and from post assignments, appointments, letters of correspondence, and issuance and termination of credential.

Disposition: Cut off upon termination of requirement for use of or termination in position requiring credential. Destroy 2 years after cutoff. **TEMPORARY**

OFFICIAL USE ONLY

Series 2: Intelligence Community Liaisons

Series Detailed Description: Includes records of liaisons with external and internal agencies in intelligence, law enforcement, security, governmental; DOE laboratories, counterintelligence field elements and NNSA to facilitate sharing intelligence information. The records can be reports, MOA, MOU, administrative correspondence intelligence information, presentations.

Item 3: Presidential Reports, external guidance, commissions and resultant action item resolutions, periodic conferences, meetings, site reviews, and requests from NNSA, field sites and DOE laboratories.

Disposition: Destroy 2 years after completion of all action item resolutions. **TEMPORARY**

Item 4: Intelligence Assessments. Final version and related source copy of each periodic report, intelligence threat assessment, intelligence memorandum or other products produced by DOE or produced for another organization for which DOE/OCI served as coordinator or chairperson.

Disposition: Destroy when record is 5 years old. **TEMPORARY**

Item 5: Liaison and Outreach to Congress, external and internal agencies through councils, working groups, task force or sub work groups.

Disposition: Destroy when record is 15 years old. **TEMPORARY**

OFFICIAL USE ONLY

Series 3: Case Files and Program Specific Files

Series Detailed Description: Investigative case files and program specific files used for counterintelligence including ongoing and completed case files of subject material or projects relating to each program's mission.

Item 6: Working Files including reports, notes, drafts, working papers and other records used, created or circulated by OCI staff in developing an intelligence threat assessment, the final case file report, intelligence publication or other product resulting from the gathered working information.

Collection of information for use as potential counterintelligence or counterterrorism value, and contact reports. Also included are the collection, publication and distribution of intelligence data including procedures, working documentation, distribution lists, intelligence threat assessment, intelligence memoranda, e-mail and reports.

Documents, submissions, substantive drafts, comments, or other records which **ARE ESSENTIAL** to the understanding of DOE/OCI's formulation and execution of policies, decisions, or programs and Requests for Information Management. (See item #10 for non-essential).

Disposition: Destroy when 15 years old. **TEMPORARY**

Item 7: Program Products including Country Information, Countries of Interest, Foreign Entities, Sensitive Technologies List, Sanctioned Entities, List CI Notes, Foreign Intelligence Threat Summaries (FITS), comprehensive assessments, counterterrorism reporting/analysis and special assessments.

Disposition: Destroy when 15 years old. **TEMPORARY**

Item 8: Correspondence on High Risk Access and Completed Access Evaluations. Includes points of contact lists, communications with high-risk program managers and security administrators, challenges to polygraph evaluations, notifications, videotapes of polygraph tests; electronic databases and spreadsheets; Issue cases, Code of Conduct letters; and access recommendations. Also included are completed Financial Analysis case files, database records review, and reports from commercial databases (Choicepoint, Autotrac, Equifax).

Disposition: Destroy when 10 years old, or when two five-year polygraph exams have been completed. **TEMPORARY**

OFFICIAL USE ONLY

Item 9: Investigative Case Files Open and Closed. Case files include inserts, correspondence both e-mail and written, threat assessment, foreign intelligence sources and indices check. Also included are special project or case files on HEU or Nuclear project program that are not electronically included in CI-EA, but identified as part of a case.

Disposition: See Item 19 for disposition. **TEMPORARY**

NOTE: **Non-electronic inserts cannot be orphaned from a case in CI-AIMS.**

Item 10: Intelligence Assessments. Working Files includes reports, notes, drafts, working papers and other records used, created or circulated by OCI staff in developing an intelligence threat assessment, final report, publication or other product. These submissions, notes, drafts, comments or other records are **NOT ESSENTIAL** to the understanding of DOE/OCI's formulation of policy. (See item #6 for essential).

Disposition: Destroy when record is 5 years old. **TEMPORARY**

Item 11: OCI Inspection documentation including working papers, logistics for site inspections (travel arrangements, equipment shipping, package wrapping), and scheduling of inspection team and inspection site.

Disposition: Destroy when record is 2 years old. **TEMPORARY**

Item 12: OCI/ODNCI Final Inspection Reports on Programs and Field Sites that include final report, findings/recommendations, responses to findings and closeout.

Disposition: Destroy when record is 10 years old. **TEMPORARY**

Item 13: Counterintelligence/Counterterrorism Working Groups and resultant documentation, intelligence publications or policy to facilitate adhering to the OCI/ODNCI mission. This includes The CT Council, CT/WMD Working Group, Combating Terrorism Intelligence WG, Foreign Terrorism Tracking Task Force (FTTF) and various working or sub-working groups in the intelligence arena.

Disposition: Destroy when record is 2 years old. **TEMPORARY**

OFFICIAL USE ONLY

Item 14: Polygraph Tests, Selection of test types, Periodic Reports, Trending Analyses, Spreadsheets and database information from CI-ACTS, CI-AIMS, CI-POLY, Scheduling Roster and logistics used to perform scheduling. Also includes lists of new and incumbent staff, contact information and scheduling calendars that facilitate processing polygraph testing.

Disposition: Destroy when record is 25 years old. **TEMPORARY**

Item 15: Final Polygraph Test Results and associated completed forms or documentation required to request and complete a polygraph test.

Disposition: Destroy when record is 25 years old. **TEMPORARY**

Item 16: Counterintelligence Course Outlines, Logistics for each course, Program Schedule of Classes (by title, by program), SCIO Conference Agenda and logistics, meeting minutes, member database for CI Awareness, attendee lists, Certificates of Completion all related to OCI/ODNCI training.

Disposition: Destroy when the record is 15 years old. **TEMPORARY**

Item 17: CARDS Database Training for data input and documentation retrieval. The training documentation includes submitted requests, scheduling logistics, completion test, certificates, comments and suggestions.

Disposition: Destroy OCI copy when 7 years old. (Note: Record to be sent to OPF when 5 years old.) **TEMPORARY**

Item 18: Documentation of polygraph test results and evaluation of Quality Control and testing processes used to facilitate performance evaluations and ensure polygraph criteria are met and adhered to as a means of evaluating staff's performance when administering polygraph testing.

Disposition: Destroy OCI copy when 25 years old. (Note: Record to be sent to OPF in blocks of 5 year-old-groups.) **TEMPORARY**

OFFICIAL USE ONLY

Series 4: Electronic Network System Processing

Series Detailed Description: Electronic database modules used by OCI programs such as Operations and Investigation, Analysis, Evaluations, Polygraph, and Inspections Programs for classified processing.

Item 19: Data that is stored in relational databases where the resultant output is in the form of documents or reports from electronic databases such as CARDS, *web*CARDS, CI-AIMS, CI-POLY, CI-EVAL, IIRs, and etcetera. Also included are database modules for processing, maintaining and updating access evaluations, financial analyses and investigations.

Hosts Briefing and Debriefing of Foreign Visitors and Assignments, and etc. These two items include initial CI briefing and documentation into CARDS.

Disposition: Destroy record when 75 years old, or when system and data are superseded or replaced, or when mission requirements dictate system obsolescence, whichever is later. **TEMPORARY**

Series 1: Program Administrative Policy and Procedure **Classified up to SECRET**

Series Detailed Description: DOE Office of Counterintelligence/Office of Nuclear Counterintelligence Administrative Correspondence including Program Policy and Procedures; Administrative Management and Procedures; Historical CI Investigation Procedures and Foreign Intelligence Administration Policy and Procedures.

Item 1: Counterintelligence Correspondence, DOE Policy, Management and Procedures, Administrative Management, Programs Administrative Records; Historical CI Investigation Procedures and Foreign Intelligence.

Disposition: Transfer to Archives' Classified Storage when record is 25 years old. **PERMANENT**

Item 2: Documentation for processing and presentation of credentials to be used in counterintelligence investigation or inspection requirements, including to and from post assignments, appointment, letters of correspondence, and issuance and termination of credential.

Disposition: Destroy when 5 years old. **TEMPORARY**

Series 2: Public Relations and Liaisons w/Agencies **Classified up to SECRET**

Series Detailed Description: Includes records of liaisons with external and internal agencies in intelligence, law enforcement, security, Congressional/ Presidential; DOE laboratories, counterintelligence field elements and NNSA to facilitate sharing intelligence information. The records can be reports, MOA, MOU, administrative correspondence intelligence information, presentations.

Item 3: Presidential Reports and Guidelines such as the HAMRE Commission, periodic conferences, meetings, site reviews, and requests from NNSA, field sites and DOE laboratories.

Disposition: Destroy when record is 2 years old. **TEMPORARY**

Item 4: Publications. Final version and related source copy of each periodic report, intelligence threat assessment, intelligence memorandum or other product produced by DOE or produced for another organization for which DOE/OCI served as coordinator or chairperson.

Disposition: Destroy when record is 5 years old. **TEMPORARY**

Item 5: Counterterrorism Liaison and Outreach to Congress, external and internal agencies through councils, working groups, task force or sub work groups.

Disposition: Destroy when record is 15 years old. **TEMPORARY**

Series 3: Case Files and Program Specific Files **Classified up to SECRET**

Series Detailed Description: Investigative case files and program specific files used for counterintelligence including ongoing and completed case files of subject material or projects relating to each program's mission.

Item 6: Publications Working Files including reports, notes, drafts, working papers and other records used, created or circulated by OCI staff in developing an intelligence threat assessment, the final case file report, publication or other product resulting from the gathered working information.

Documents, submissions, substantive drafts, comments, or other records which are essential to the understanding of DOE/OCI's formulation and execution of policies, decisions, or programs and Requests for Information Management.

Disposition: Destroy when 15 years old. **TEMPORARY**

Item 7: Program Products including Country Information, Countries of Interest, Foreign Entities, Sensitive Technologies List, Sanctioned Entities, List CI Notes, Foreign Intelligence Threat Summaries (FITS), comprehensive assessments, counterterrorism reporting/analysis and special assessments.

Disposition: Destroy when 15 years old. **TEMPORARY**

Item 8: Correspondence on High Risk Access and Completed Access Evaluations. Includes points of contact lists, communications with high-risk program managers and security administrators, challenges to polygraph evaluations, notifications, videotapes of polygraph tests; electronic databases and spreadsheets; Issue cases, Code of Conduct letters; and access recommendations. Also included are completed Financial Analysis case files, database records review, and reports from commercial databases (Choicepoint, Autotrac, Equifax).

Disposition: Destroy when 25 years old. **TEMPORARY**

Item 9: Investigative Case Files Open and Closed. Case files include inserts, correspondence both e-mail and written, threat assessment, foreign intelligence sources and indices check. Also included are special project or case files on HEU or Nuclear project program.

Disposition: Destroy each closed individual case file when 15 years old. **TEMPORARY**

Item 10: Final documentation of Hosts Briefing, Hosts Debriefing of Foreign Visitors and Assignees and the resultant Intelligence Information Reports (IRR). These three items include initial CI briefing, documentation into CARDS, and collection of information for use of potential counterintelligence or counterterrorism value, and contact reports. Also included are the collection, publication and distribution of intelligence data including procedures, working documentation, distribution lists, intelligence threat assessment, intelligence memoranda, e-mail and reports.

Disposition: Transfer to Archives' Classified Storage when record is 15 years old. **PERMANENT**

Item 11: Publications Working Files includes reports, notes, drafts, working papers and other records used, created or circulated by OCI staff in developing an intelligence threat assessment, final report, publication or other product. These submissions, notes, drafts, comments or other records are NOT essential to the understanding of DOE/OCI's formulation of policy.

Disposition: Destroy when record is 10 years old. **TEMPORARY**

Item 12: OCI Inspection documentation including working papers, logistics for site inspections (travel arrangements, equipment shipping, package wrapping), and scheduling of inspection team and inspection site.

Disposition: Destroy when record is 2 years old. **TEMPORARY**

Item 13: OCI/ODNCI Final Inspection Reports on Programs and Field Sites that include final report, findings/recommendations, responses to findings and closeout.

Disposition: Destroy when record is 10 years old. **TEMPORARY**

Item 14: Counterintelligence/Counterterrorism Working Groups and resultant documentation, publications or policy to facilitate adhering to the OCI/ODNCI mission. This includes The CT Council, CT/WMD Working Group, Combating Terrorism Intelligence WG, Foreign Terrorism Tracking Task Force (FTTF) and various working or sub-working groups in the intelligence arena.

Disposition: Destroy when record is 2 years old. **TEMPORARY**

Item 15: Polygraph Tests, Selection of test types, Periodic Reports, Trending Analyses, Spreadsheets and database information from CI-ACTS, CI-AIMS, CI-POLY, Scheduling Roster and logistics used to perform scheduling. Also includes lists of new and incumbent staff, contact information and scheduling calendars that facilitate processing polygraph testing.

Disposition: Destroy when record is 25 years old. **TEMPORARY**

Item 16: Final Polygraph Test Results and associated completed forms or documentation required to request and complete a polygraph test.

Disposition: Destroy when record is 25 years old. **TEMPORARY**

Item 17: Counterintelligence Course Outlines, Logistics for each course, Program Schedule of Classes (by title, by program), SCIO Conference Agenda and logistics, meeting minutes, member database for CI Awareness, attendee lists, Certificates of Completion all related to OCI/ODNCI training.

Disposition: Destroy when the record is 15 years old. **TEMPORARY**

Item 18: CARDS Database Training for data input and documentation retrieval. The training documentation includes submitted requests, scheduling logistics, completion test, certificates, comments and suggestions.

Disposition: Destroy when OCI copy when 7 years old. (Note: Record to be sent to OPF when 5 years old.) **TEMPORARY**

Item 19: Documentation of polygraph test results and evaluation of Quality Control and testing processes used to facilitate performance evaluations and ensure polygraph criteria are met and adhered to as a means of evaluating staff's performance when administering polygraph testing.

Disposition: Destroy OCI copy when 7 years old. (Note: Record to be sent to OPF when 5 years old.) **TEMPORARY**

Series 4: Reporting and Distribution of CI Products **Classified up to SECRET**

Series Detailed Description: Final documentation of intelligence products in the form of Periodic Reports, Trending Analyses, publications of both internal and external liaisons such as IIR, GAO, Cox Report, Espionage Open Source Articles, Collection and Threat Publications.

Item 20: Threat Assessment reference documentation and administrative correspondence used in the daily processing of intelligence information. This includes copies of memoranda, reports, publications, and other working documentation maintained for reference purposes. Also may include CT Threat Assessments, Risk and Vulnerabilities from all OCI/ODNCI sites.

Disposition: Destroy when record is 2 years old. **TEMPORARY**

Series 5: Electronic Network System Processing **Classified up to SECRET**

Series Detailed Description: Electronic CI-NET Database modules used by OCI programs such as Operations and Investigation, Analysis, Evaluations, Inspections and Polygraph Programs for classified processing. Additional database, Counterintelligence Analytical Research Data System (CARDS) also used in conjunction with CI-NET to facilitate mission essential documentation.

Item 21: Database output that results in documents or reports from electronic databases such as CARDS, *web*CARDS, CI-AIMS, CI-POLY, CI-EVAL, and etcetera; database modules for processing, maintaining and updating access evaluations, financial analyses and financial investigations; spreadsheets; and logistical information.

Network, databases, spreadsheet applications and correspondence pertaining to processing classified documentation. Includes database infrastructure that supports investigative case management, research and analysis, security, evaluations, inspections, access and other applications for counterintelligence usage.

ER 7APR05 EMAIL WITH JAY BLEWETT.

Disposition: Destroy when record is 15 years old, or when system and data files are superseded or replaced, whichever is sooner. **TEMPORARY**

ELECTRONIC MAIL AND WORD PROCESSING. 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 OTHER ITEMS IN THIS SCHEDULE. ALSO INCLUDES ELECTRONIC COPIES OF RECORDS CREATED ON ELECTRONIC MAIL AND WORD PROCESSING SYSTEMS THAT ARE MAINTAINED FOR UPDATING, REVISION, OR DISSEMINATION.

a) COPIES THAT HAVE NO FURTHER ADMINISTRATIVE VALUE AFTER THE RECORDKEEPING COPY IS MADE. INCLUDES COPIES ~~MADE~~ MAINTAINED BY INDIVIDUALS IN PERSONAL FILES, PERSONAL ELECTRONIC MAIL DIRECTORIES, OR OTHER PERSONAL DIRECTORIES ON HARD DISK OR NETWORK DRIVES, AND COPIES ON SHARED NETWORK DRIVES THAT ARE USED ONLY TO PRODUCED THE RECORDKEEPING COPY.

ITEM 22: → DESTROY/DELETE WITHIN 180 DAYS AFTER THE RECORDKEEPING COPY HAS BEEN PRODUCED.

b.) COPIES USED FOR DISSEMINATION, REVISION, OR UPDATING THAT ARE MAINTAINED IN ADDITION TO THE RECORDKEEPING COPY.

ITEM 23: →DESTROY/DELETE WHEN DISSEMINATION, REVISION, OR UPDATING IS COMPLETED.

OFFICIAL USE ONLY
Contains Circumvention of Statute Information. Department of Energy approval required prior to public release.
Reviewed by: Claudia Williams

Department of Energy
Electronic Information System Questionnaire

Point of Contact (Name & Title): 1) Anthony Bailey, Chief Information Officer/Program Records Officer Office of Counterintelligence (OCI) 2) Claudia Williams, Records Liaison Officer, OCI	**Telephone Number: (202) 586-1721** **(202) 586-8924** **E-Mail Address:** **Anthony.Bailey@cn.doe.gov** **Claudia.Williams@cn.doe.gov**
DOE Program / Location: Office of Counterintelligence/FORS Bldg.	**Date Submitted: October 12, 2004**
Is this Schedule: ☑ **DOE-Wide** ☐ **Site Specific**	**Inclusive Dates:** February 1998 to Infinity
Access Restrictions (if any):	**Categories:** ☐ Epidemiology ☐ Quality Assurance ☐ Privacy Act ☑ Vital Records ☐ Other (specify)

1. **What is the name of the system (both acronym and full)? The Counterintelligence Enterprise Applications (CI-EA). The CI-EA is comprised of the following subsystems:**
   a) Counterintelligence Access Control Tracking System (CI-ACTS)
   b) Counterintelligence Analytical Research Data System (CARDS → *web*CARDS)[1]
   c) Counterintelligence Automated Investigative Management System (CI-AIMS)
   d) Counterintelligence Polygraph System (CI-POLY)
   e) Counterintelligence Evaluation System (CI-EVAL)

2. **What is the name of the program office responsible for this system?**
   Office of Counterintelligence.

3. **What is the program/legal authority for the creation of the system?**
   EO 12333, PDD-61.

[1] *web*CARDS will be the web-based implementation of the current CARDS database application.

4. **What is the purpose of the system? The CI-EA is a tightly integrated system with** built-in access controls and many instances of reusable Oracle database tables. The CI-EA subsystems are used for various functions that support the mission of the OCI. Details of each subsystem are provided in the sections below. Many of these data sets are shared by the five subsystems. For example, user information is tied directly to cases that are inputted into CI-AIMS, *web*CARDS, CI-POLY, or CI-EVAL. Another example of information that is shared among the subsystems include, but are not limited to, information on foreign travelers who visit DOE sites that are captured in CARDS/*web*CARDS and may later be used in a case in CI-AIMS, CI-POLY, or CI-EVAL, DOE employees who perform official travel to foreign countries, etcetera.

Counterintelligence Access Control Tracking System (**CI-ACTS**)

CI-ACTS automates the processing of Counterintelligence personnel into the Department of Energy Counterintelligence programs. This database application also serves as a 'traffic cop' for controlling access to the CI-EA. Users may log into CI-ACTS (or any of the CI-EA applications) using a token for authentication. After single authentication users gain access to all CI-EA applications based on a pre-defined role.

Counterintelligence Analytical Research Data System

The CARDS application is a centralized database application used by OCI for collecting counterintelligence information. It serves as a repository of counterintelligence data used to detect, track and analyze the foreign intelligence threat to DOE personnel and programs. CARDS will collect information to assist briefers in sensitizing DOE managers and personnel to specific foreign intelligence service trends and activities. The system will also help track associations among DOE personnel and foreign nationals.

Counterintelligence Automated Investigative Management System (**CI-AIMS**)

The Counterintelligence Administrative Investigations Management System (CI-AIMS) application is an automated, easy-to-use, web-browser based system for the entry, access, *routing and approval,* referral, review and reporting of centralized, Administrative Investigation file information, by privileged Investigators and Investigative Program support personnel, at DOE Headquarters and in the field. CI-AIMS provides simple-to-use, yet powerful methods for relating multiple subjects, inserts, and documents to an Administrative Investigation file, tracking CI Officers assigned to the investigation, and for the management of Administrative Investigation file approvals, referrals, reports, and reviews.

CI-AIMS provides CI support personnel, with the appropriate privileges, the ability to initiate, search, retrieve, update, and track Administrative Investigations through each stage of the approval process, from initiation to closure. CI-AIMS integrated workflow automates the approval process required by law to conduct Administrative Investigations. CI-AIMS integrated workflow *routes* Administrative Investigation files for approval automatically from the initiating field CIO to the Senior Field CIO for Preliminary Inquiry approvals and from the Senior Field CIO to the Desk Officer, Director or Deputy Director of the Investigations Program at Headquarters for Administrative Investigations approvals. CI-AIMS tracks route history,

informs privileged users of location and status of Administrative Investigation files within the approval process, sends alerts regarding upcoming due dates and expirations, and provides for the customization of automated routes by privileged users. CI-AIMS likewise provides for the initiation, assignment, and control of leads, from within Headquarters, from Sr. CIO to Sr. CIO in the field, and from Sr. CIO to CIO within a location.

CI-AIMS enforces the security required by law to protect Administrative Investigation file and subject information. CI-AIMS access controls restrict access to secure Counterintelligence Administrative Investigation files to those individuals with express need-to-know access requirements. With security enforced at the record level, searches of the CI-AIMS database will return those specific Administrative Investigation file records that the Counterintelligence Investigator, or support personnel, has the privilege to see. In response to Headquarters specific requests, a global ""Administrative Investigation file index"" search capability enables only those appropriately privileged users to verify the existence of an Administrative Investigation file. Additional, record-level privileges would be required to further review the Administrative Investigation file or access details.

CI-AIMS provides Counterintelligence Investigators, and support personnel, with the ability to enter, search, retrieve and update Administrative Investigation file information, building relationships among Administrative Investigation components useful to the investigative process.

The CI-AIMS unique, system-generated, Administrative Investigation file number, coupled with the automatically generated prefix, identifies an Administrative Investigation at all stages of processing, from initiation, authorization, to referral (if required) and final closure. All of the collective documents within an Administrative Investigation file are retrieved and managed by the system using the unique Administrative Investigation file number and prefix. The Administrative Investigation file number links Administrative Investigations to inserts, leads, subject profiles, assigned officers, reviews, referrals, approvals, reports, and documents.

CI-AIMS automates, records, and tracks the history of an Administrative Investigation, including case file initiation, approval and authorizations, the escalation of administrative inquiries, lead assignment, inserts, the entry of subject information and evidentiary documents, records of periodic file reviews, reports, referrals and final closure authorization. CI-AIMS Administrative Investigation information content is managed logically, as it would be in any file system, paper-based or electronic. For example, within an Administrative Investigation file, there can be many inserts, so logically, the system relates one Administrative Investigation record to many insert records. Many subjects may be a part of an Administrative Investigation, so logically the system links an Administrative Investigation record to many subject records. Within the CI-AIMS application, in addition to other multi-value fields (e.g., languages, skills, etc.,) multiple lists of addresses, AKAs, associated individuals (specifying type and citizenship), phone numbers, and images may be related to a single subject. Within Counterintelligence, there may be many Counterintelligence Officers (CIOs) working on a case; CI-AIMS tracks all CIOs having access to the case, for approval and authorization, lead assignments, and insert activities.

Counterintelligence Polygraph System (**CI-POLY**)

The CI-POLY application provides the capability for the polygraph examiners to automate and store polygraph examinations. This set of information includes the scheduling of the exam;

electronically storing the appropriate consent forms, audio/video session, related charts, and examiners comments, as well as quality control processes. In addition to storing polygraph examination information, the CI-POLY database application provides a mechanism for the Polygraph Program to provide supporting data to the Counterintelligence Evaluation Program personnel who are charged with the vetting of DOE personnel who require DOE Q clearances, access to special access and high risk programs.

Counterintelligence Evaluation System (**CI-EVAL**)

The CI-EVAL database application automates the processes that are used by the Counterintelligence Evaluation Program to complete the vetting process for DOE personnel who require DOE Q clearances, SCI access, and access to special programs such as SAP, HRP, and etcetera.

5. **What are the source(s) of input for these systems?**
   Assigned administrative support staff functional area personnel, scanned documents, automated audio/video captures, and imported data from other sources.

6. **What are the applications this system supports (how are the data manipulated once they have been input)?**
   The applications supported include all areas of the Office of Counterintelligence. The data is manipulated in several ways once the data has been recorded. The following is an example based on the specific database application:

CI-ACTS:	Data is used to track CI personnel who enter and leave the program.
CARDS → *web*CARDS:	Data is manipulated to provide statistics on briefings/debriefings, visits and assignments, and etcetera.
CI-AIMS:	Data used for tracking CI investigations. Information also used to make referrals to law enforcement agencies, reports to Congress, and etcetera.
CI-POLY:	This type of data is used to record polygraph examination results. Statistical data also used in support of reports prepared for Congress and other federal bodies as required.
CI-EVAL:	Used for vetting of employees who require special accesses and clearances. Also used for input for reports to Congress

7. **What are the outputs from this system?**
   Reports, statistical information, intelligence information dissemination, law enforcement case referrals to agencies such as the FBI, CIA, and etcetera.

8. **What is the primary key/unit of analysis for each file (one record is created for each)?**
   The primary key/unit for each file depends on the application and its usage. For example, case information that is stored in CI-AIMS has a primary key/unit of analysis that is based on a uniquely identified case number. The associated information that comprises this case (i.e. documents, scanned information, video/audio files, etcetera) is stored in Oracle tables and are linked based on the case ID number. Since these suite of applications reside in a relational database infrastructure, records are created on an ad hoc basis, as well as individual reports based on the need of DOE, Congress, law enforcement agencies, and etcetera.

9. **What documentation is available for this system?**
   Complete design and operational documents for all phases of implementation are available. The program staff also maintains documentation of the changes made to the system design.

10. **What are the inclusive dates for the file(s)?**
    The dates begin with inception of this Program Office, February 1998 and expected to continue throughout the lifespan of the Office of Counterintelligence or disposition rules specified in the Office of Counterintelligence Records Schedule.

11. **Are the records in this system necessary to protect the rights or interests of the Government or individuals affected by the Government (vital records)?**
    Yes. The vital records will be identified on both the OCI Records Schedule and File Plan.

12. **Are there any restrictions on the release to the public of the data? If yes, please cite the authority for those restrictions. If yes, can any segregable portions of the file be released or does the system produce a public use version of the data?**
    Yes. Privacy Act of 1974, various PDDs (24, 61, 63), EO 12333. Unclassified information outputted from the system can be segregated and released as public version if required.

13. **Would data or outputs from this system be likely subjects of Freedom of Information Act Requests?**
    Yes.

14. **Would portions of the data be lost or distorted upon conversion to flat file format (ASCII or EBCDIC)?**
    Not necessarily. This depends on the data that is requested as well as the dependencies of the system.

15. What hardware is used for this system?
The hardware used for this system includes TACLANE Type I bulk encryptors, RSA tokens (used for authentication) Sun servers, Intel-based servers, user workstations, printers, scanners, network attached storage devices, and other input devices.

16. What software is used for this system?
The software used for this system is comprised of Oracle database management system, Report software, Cold Fusion, Solaris operating systems, Microsoft Windows operating systems (server and client), SQL Windows, web browser, system/application management software, and other software used to support hardware devices such as scanners, printers, and other input devices.

17. Does the system have a privacy act listing?
No.

18. Recommended disposition for electronic data.
The disposition for electronic data is defined in the OCI records schedule. See item #20.

19. Recommended disposition for outputs.
Destroy when no longer required for business or operational purposes.

20. Recommended disposition for input data sources.
Destroy when no longer required for business or operational purposes, except in cases where hard copies (such as documents with signatures) are required by statute or regulation.

21. Recommended disposition for system documentation.
Destroy when databases are 10,000 years old, or when system and data are superseded, replaced or when mission requirements dictate obsolescence.

Concurrence:

1. Program Records Official _____ Date _____
   Anthony Z. S. Bailey
2. General Counsel _____ Date _____
3. Departmental Records Officer _____ Date _____
   Sharon A. Evelin

Department of Energy
Electronic Information System Questionnaire

Point of Contact (Name & Title): 1) Anthony Bailey, Chief Information Officer/Program Records Officer Office of Counterintelligence (OCI) 2) Claudia Williams, Records Liaison Officer, OCI	**Telephone Number:** (202) 586-1721 (202) 586-8924 **E-Mail Address:** Anthony.Bailey@cn.doe.gov Claudia.Williams@cn.doe.gov
DOE Program / Location: Office of Counterintelligence/FORS Bldg.	**Date Submitted: October 12, 2004**
Is this Schedule: ☑ **DOE-Wide** ☐ **Site Specific**	**Inclusive Dates:** February 1998 to Infinity
Access Restrictions (if any):	**Categories:** ☐ Epidemiology ☐ Quality Assurance ☐ Privacy Act ☑ Vital Records ☐ Other (specify)

1. **What is the name of the system (both acronym and full)? The Counterintelligence Enterprise Applications (CI-EA). The CI-EA is comprised of the following subsystems:**
   a) Counterintelligence Access Control Tracking System (CI-ACTS)
   b) Counterintelligence Analytical Research Data System (CARDS → *web*CARDS)[1]
   c) Counterintelligence Automated Investigative Management System (CI-AIMS)
   d) Counterintelligence Polygraph System (CI-POLY)
   e) Counterintelligence Evaluation System (CI-EVAL)

2. **What is the name of the program office responsible for this system?**
   Office of Counterintelligence

3. **What is the program/legal authority for the creation of the system?**
   EO 12333, PDD-61

4. **What is the purpose of the system?** The CI-EA is a tightly integrated system with built-in access controls and many instances of reusable Oracle database tables. The CI-EA subsystems are used for various functions that support the mission of the OCI. Details of each subsystem are provided in the sections below. Many of these data sets are shared by the five subsystems. For example, user information is tied directly to cases that are inputted into CI-AIMS, *web*CARDS, CI-POLY, or CI-EVAL. Another example of information that is shared among the subsystems include, but are not limited to, information on foreign travelers who visit DOE sites that are captured in

[1] *web*CARDS will be the web-based implementation of the current CARDS database application.

CARDS/*web*CARDS and may later be used in a case in CI-AIMS, CI-POLY, or CI-EVAL, DOE employees who perform official travel to foreign countries, etcetera.

Counterintelligence Access Control Tracking System (**CI-ACTS**)

CI-ACTS automates the processing of Counterintelligence personnel into the Department of Energy Counterintelligence programs. This database application also serves as a 'traffic cop' for controlling access to the CI-EA. Users may log into CI-ACTS (or any of the CI-EA applications) using a token for authentication. After single authentication users gain access to all CI-EA applications based on a pre-defined role.

Counterintelligence Analytical Research Data System

The CARDS application is a centralized database application used by OCI for collecting counterintelligence information. It serves as a repository of counterintelligence data used to detect, track and analyze the foreign intelligence threat to DOE personnel and programs. CARDS will collect information to assist briefers in sensitizing DOE managers and personnel to specific foreign intelligence service trends and activities. The system will also help track associations among DOE personnel and foreign nationals.

Counterintelligence Automated Investigative Management System (**CI-AIMS**)

The Counterintelligence Administrative Investigations Management System (CI-AIMS) application is an automated, easy-to-use, web-browser based system for the entry, access, *routing and approval*, referral, review and reporting of centralized, Administrative Investigation file information, by privileged Investigators and Investigative Program support personnel, at DOE Headquarters and in the field. CI-AIMS provides simple-to-use, yet powerful methods for relating multiple subjects, inserts, and documents to an Administrative Investigation file, tracking CI Officers assigned to the investigation, and for the management of Administrative Investigation file approvals, referrals, reports, and reviews.

CI-AIMS provides CI support personnel, with the appropriate privileges, the ability to initiate, search, retrieve, update, and track Administrative Investigations through each stage of the approval process, from initiation to closure. CI-AIMS integrated workflow automates the approval process required by law to conduct Administrative Investigations. CI-AIMS integrated workflow *routes* Administrative Investigation files for approval automatically from the initiating field CIO to the Senior Field CIO for Preliminary Inquiry approvals and from the Senior Field CIO to the Desk Officer, Director or Deputy Director of the Investigations Program at Headquarters for Administrative Investigations approvals. CI-AIMS tracks route history, informs privileged users of location and status of Administrative Investigation files within the approval process, sends alerts regarding upcoming due dates and expirations, and provides for the customization of automated routes by privileged users. CI-AIMS likewise provides for the initiation, assignment, and control of leads, from within Headquarters, from Sr. CIO to Sr. CIO in the field, and from Sr. CIO to CIO within a location.

CI-AIMS enforces the security required by law to protect Administrative Investigation file and subject information. CI-AIMS access controls restrict access to secure Counterintelligence Administrative Investigation files to those individuals with express need-to-know access requirements. With security enforced at the record level, searches of the CI-AIMS database will

return those specific Administrative Investigation file records that the Counterintelligence Investigator, or support personnel, has the privilege to see. In response to Headquarters specific requests, a global ""Administrative Investigation file index"" search capability enables only those appropriately privileged users to verify the existence of an Administrative Investigation file. Additional, record-level privileges would be required to further review the Administrative Investigation file or access details.

CI-AIMS provides Counterintelligence Investigators, and support personnel, with the ability to enter, search, retrieve and update Administrative Investigation file information, building relationships among Administrative Investigation components useful to the investigative process.

The CI-AIMS unique, system-generated, Administrative Investigation file number, coupled with the automatically generated prefix, identifies an Administrative Investigation at all stages of processing, from initiation, authorization, to referral (if required) and final closure. All of the collective documents within an Administrative Investigation file are retrieved and managed by the system using the unique Administrative Investigation file number and prefix. The Administrative Investigation file number links Administrative Investigations to inserts, leads, subject profiles, assigned officers, reviews, referrals, approvals, reports, and documents.

CI-AIMS automates, records, and tracks the history of an Administrative Investigation, including case file initiation, approval and authorizations, the escalation of administrative inquiries, lead assignment, inserts, the entry of subject information and evidentiary documents, records of periodic file reviews, reports, referrals and final closure authorization. CI-AIMS Administrative Investigation information content is managed logically, as it would be in any file system, paper-based or electronic. For example, within an Administrative Investigation file, there can be many inserts, so logically, the system relates one Administrative Investigation record to many insert records. Many subjects may be a part of an Administrative Investigation, so logically the system links an Administrative Investigation record to many subject records. Within the CI-AIMS application, in addition to other multi-value fields (e.g., languages, skills, etc.,) multiple lists of addresses, AKAs, associated individuals (specifying type and citizenship), phone numbers, and images may be related to a single subject. Within Counterintelligence, there may be many Counterintelligence Officers (CIOs) working on a case; CI-AIMS tracks all CIOs having access to the case, for approval and authorization, lead assignments, and insert activities.

Counterintelligence Polygraph System (**CI-POLY**)

The CI-POLY application provides the capability for the polygraph examiners to automate and store polygraph examinations. This set of information includes the scheduling of the exam; electronically storing the appropriate consent forms, audio/video session, related charts, and examiners comments, as well as quality control processes. In addition to storing polygraph examination information, the CI-POLY database application provides a mechanism for the Polygraph Program to provide supporting data to the Counterintelligence Evaluation Program personnel who are charged with the vetting of DOE personnel who require DOE Q clearances, access to special access and high risk programs.

Counterintelligence Evaluation System (**CI-EVAL**)

The CI-EVAL database application automates the processes that are used by the Counterintelligence Evaluation Program to complete the vetting process for DOE personnel who

require DOE Q clearances, SCI access, and access to special programs such as SAP, HRP, and etcetera.

5. **What are the source(s) of input for these systems?**
   Assigned administrative support staff functional area personnel, scanned documents, automated audio/video captures, and imported data from other sources.

6. **What are the applications this system supports (how are the data manipulated once they have been input)?**
   The applications supported include all areas of the Office of Counterintelligence. The data is manipulated in several ways once the data has been recorded. The following is an example based on the specific database application:

CI-ACTS:	Data is used to track CI personnel who enter and leave the program.
CARDS → *web*CARDS:	Data is manipulated to provide statistics on briefings/debriefings, visits and assignments, and etcetera.
CI-AIMS:	Data used for tracking CI investigations. Information also used to make referrals to law enforcement agencies, reports to Congress, and etcetera.
CI-POLY:	This type of data is used to record polygraph examination results. Statistical data also used in support of reports prepared for Congress and other federal bodies as required.
CI-EVAL:	Used for vetting of employees who require special accesses and clearances. Also used for input for reports to Congress

7. **What are the outputs from this system?**
   Reports, statistical information, intelligence information dissemination, law enforcement case referrals to agencies such as the FBI, CIA, and etcetera.

8. **What is the primary key/unit of analysis for each file (one record is created for each)?**
   The primary key/unit for each file depends on the application and its usage. For example, case information that is stored in CI-AIMS has a primary key/unit of analysis that is based on a uniquely identified case number. The associated information that comprises this case (i.e. documents, scanned information, video/audio files, etcetera) is stored in Oracle tables and are linked based on the case ID number. Since these suite of applications reside in a relational database infrastructure, records are created on an ad hoc basis, as well as individual reports based on the need of DOE, Congress, law enforcement agencies, and etcetera.

9. **What documentation is available for this system?**
Complete design and operational documents for all phases of implementation are available. The program staff also maintains documentation of the changes made to the system design.

10. **What are the inclusive dates for the file(s)?**
The dates begin with inception of this Program Office, February 1998 and expected to continue throughout the lifespan of the Office of Counterintelligence or disposition rules specified in the Office of Counterintelligence Records Schedule.

11. **Are the records in this system necessary to protect the rights or interests of the Government or individuals affected by the Government (vital records)?**
Yes. The vital records will be identified on both the OCI Records Schedule and File Plan.

12. **Are there any restrictions on the release to the public of the data? If yes, please cite the authority for those restrictions. If yes, can any segregable portions of the file be released or does the system produce a public use version of the data?**
Yes. Privacy Act of 1974, various PDDs (24, 61, 63), EO 12333. Unclassified information outputted from the system can be segregated and released as public version if required.

13. **Would data or outputs from this system be likely subjects of Freedom of Information Act Requests?**
Yes.

14. **Would portions of the data be lost or distorted upon conversion to flat file format (ASCII or EBCDIC)?**
Not necessarily. This depends on the data that is requested as well as the dependencies of the system.

15. **What hardware is used for this system?**
The hardware used for this system includes TACLANE Type I bulk encryptors, RSA tokens (used for authentication) Sun servers, Intel-based servers, user workstations, printers, scanners, network attached storage devices, and other input devices.

16. **What software is used for this system?**
The software used for this system is comprised of Oracle database management system, Report software, Cold Fusion, Solaris operating systems, Microsoft Windows operating systems (server and client), SQL Windows, web browser, system/application management software, and other software used to support hardware devices such as scanners, printers, and other input devices.

17. **Does the system have a privacy act listing?**
No.

18. Recommended disposition for electronic data.
The disposition for electronic data is defined in the OCI records schedule. See item #21.

19. Recommended disposition for outputs.
Destroy when no longer required for business or operational purposes.

20. Recommended disposition for input data sources.
Destroy when no longer required for business or operational purposes, except in cases where hard copies (such as documents with signatures) are required by statute or regulation.

21. Recommended disposition for system documentation.

a. Revisions -- Cutoff when superceded or revised. See OCI records schedule item #21.

b. Final System Documentation -- Transfer the final version of the documentation to NARA with the data files and system after the system is superseded or replaced, see OCI records schedule item #21.

Concurrence:

1. Program Records Official _____ Date _____
2. General Counsel _____ Date _____
3. Departmental Records Officer _____ Date _____

DOE F 243.1
10/00

REPLACES DOE F 1324.5

U.S. DEPARTMENT OF ENERGY
RECORDS SCHEDULE WORKSHEET

Instructions: This Form Must Accompany Proposed SF-115

1. Point of Contact (Name and Title):
Anthony Bailey, Chief Information Officer, Office of Counterintelligence

3. Telephone No.: **(202) 586-1721**

4. E-Mail Address: **Anthony.Bailey@cn.doe.gov**

2. DOE Site and Organization Title:
Office of Counterintelligence, CN-1

5. Date Submitted: **01/14/2005**

6. Schedule: (Series will apply to more than one site)
Generic ☐ Site Specific ☒

7. Identify Related Schedules(s):
N/A

8. Series Title and Description: (Indicate function/purpose of information. For electronic records include: System description, input and output source, and metadata.)

This schedule has five series. Each series title and its description are outlined on the Continuation Page for this Item No. 8.

☒ See Continuation Page (Attach Blank Sheet)

9. Related Records (Explain reason for any duplication of recordkeeping, relationship of related records to record series, and disposition periods, if different from Item 13).

10. Record Medium:
☒ Paper
☐ Microfilm
☒ Audiovisual
☐ Electronic: Hardware/ Software Environment: _____
☐ Other, Specify _____

11. Categories:
☐ Epidemiology
☐ Quality Assurance
☐ Vital Records
☐ Emergency Operating
☒ Rights & Interests
☐ Privacy Act
☐ Other, Specify _____

12. Reference Activity:
☒ Active (At least once a month per file unit)
☐ Semi-Active (Less than once a month per file unit)
☐ Inactive (Not used for current agency/business)

13. Recommended Disposition Period:
See Attached Draft Counterintelligence Records Schedule

14. Justification (Includes regulatory drivers):

15. File Cutoff Instructions:
☐ 1 Month
☐ 1 Year
☐ 6 months
☒ Other, Specify: **Various**

16. Condition of Records:
Good, clean and dry.

17. Files Arranged by: (Check appropriate boxes):
☐ Subject
☐ Case
☐ Numerically
☐ Chronologically
☐ Alphabetically
☒ Other, Specify: **All arrangements used.**

18. Inclusive Dates: (Leave blank if specific dates unknown)
02/01/1998 (From)
01/14/2005 (To)

19. Total Volume
Electronic (Cubic Feet)

20. Annual Accumulation
Electronic (Cubic Feet)

21. Restrictions on Access:
☐ Unclassified
☒ Restrictions, Specify: **Classified**

22. Location of Records (Bldg/Room No.):
Office of Counterintelligence, Forrestal Bldg. (3rd, Ground and 8th floors)

23. Concurrence for Program, Legal, Other: (Name, Organization and Date):

a. **Claudia Williams, Records Liaison Officer** **01/14/2005**

b. _____

c. _____

DOE F 243.1 Records Schedule Worksheet
Continuation Page

Item No. 8:

Series1: Program Administrative Policy and Procedures

DOE Office of Counterintelligence/Office of Nuclear Counterintelligence Administrative Correspondence including Program Policy and Procedures; Administrative Management and Procedures; historical CI Investigation Procedures and Foreign Intelligence Administration Policy and Procedures.
CLASSIFIED UP TO SECRET

Series 2: Public Relations and Liaisons w/Agencies

Includes records of liaisons with external and internal agencies in intelligence, law enforcement, security, Congressional/Presidential; DOE laboratories, counterintelligence field elements and NNSA to facilitate sharing intelligence information. The records can be reports, MOA, MOU, administrative correspondence, intelligence information or presentations.
CLASSIFIED UP TO SECRET

Series 3: Case Files and Program Specific Files

Investigative case files and program specific files used for counterintelligence including ongoing and completed case files of subject material or projects relating to each program's mission.
CLASSIFIED UP TO SECRET

Series 4: Reporting and Distribution of CI Products

Final documentation of intelligence products in the form of Periodic Reports, Trending Analyses, publications of both internal and external liaisons such as IIR, GAO, Cox Report, Espionage Open Source Articles, Collection and Threat Publications.
CLASSIFIED UP TO SECRET

Series 5: Electronic Network System Processing

Electronic CI-NET Database modules used by OIC programs such as Operations and Investigations, Analysis, Evaluations, Inspections and Polygraph Programs for classified processing. Additional database, Counterintelligence Analytical Research Data systems (CARDS) also used in conjunction with CI-NET to facilitate mission essential documentation.
CLASSIFIED UP TO SECRET